CA ARCserve® Backup für Windows

Agent für virtuelle Rechner – Handbuch

r16



CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden CA Technologies-Produkte:

- BrightStor® Enterprise Backup
- CA Antivirus
- CA ARCserve® Assured Recovery™
- CA ARCserve® Backup Agent für Advantage™ Ingres®
- CA ARCserve® Backup Agent für Novell Open Enterprise Server für Linux
- CA ARCserve® Backup Agent for Open Files für Windows
- CA ARCserve® Backup Client Agent für FreeBSD
- CA ARCserve® Backup Client Agent für Linux
- CA ARCserve® Backup Client Agent für Mainframe Linux
- CA ARCserve® Backup Client Agent für UNIX
- CA ARCserve® Backup Client Agent für Windows
- CA ARCserve® Backup Enterprise Option für AS/400
- CA ARCserve® Backup Enterprise Option für Open VMS
- CA ARCserve® Backup für Linux Enterprise Option für SAP R/3 für Oracle
- CA ARCserve® Backup für Microsoft Windows Essential Business Server
- CA ARCserve® Backup für UNIX Enterprise Option für SAP R/3 für Oracle
- CA ARCserve® Backup für Windows
- CA ARCserve® Backup für Windows Agent für IBM Informix
- CA ARCserve® Backup für Windows Agent für Lotus Domino
- CA ARCserve® Backup für Windows Agent für Microsoft Exchange Server
- CA ARCserve® Backup für Windows Agent für Microsoft SharePoint Server
- CA ARCserve® Backup für Windows Agent für Microsoft SQL Server
- CA ARCserve® Backup für Windows Agent für Oracle
- CA ARCserve® Backup für Windows Agent für Sybase
- CA ARCserve® Backup für Windows Agent für virtuelle Rechner
- CA ARCserve® Backup für Windows Disaster Recovery Option
- CA ARCserve® Backup für Windows Enterprise Module

- CA ARCserve® Backup für Windows Enterprise Option für IBM 3494
- CA ARCserve® Backup für Windows Enterprise Option für SAP R/3 für Oracle
- CA ARCserve® Backup für Windows Enterprise Option für StorageTek ACSLS
- CA ARCserve® Backup für Windows Image Option
- CA ARCserve® Backup für Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup für Windows NDMP NAS Option
- CA ARCserve® Backup für Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup für Windows Tape Library Option
- CA ARCserve® Backup Patch Manager
- CA ARCserve® Backup UNIX und Linux Data Mover
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby
- CA ARCserve® D2D
- CA ARCserve® D2D On Demand
- CA ARCserve® High Availability
- CA ARCserve® Replizierung
- CA VM: Band für z/VM
- CA 1® Bandverwaltung
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

CA Kontaktieren

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- Umbenannt auf CA Technologies.
- Thema zur Fehlersuche wurde hinzugefügt -- Es kommt zu Lizenzfehlern, wenn virtuelle Rechner gesichert und wiederhergestellt werden (siehe Seite 168).
- Das Dokument wurde mit Benutzer-Feedback, Verbesserungen, Korrekturen und anderen kleineren Änderungen aktualisiert, um die Verwendung und das Produktverständnis oder die Dokumentation selbst zu verbessern.

Inhalt

Kapitel 3: Auffüllen der CA ARCserve Backup-Datenbank 69

Kapitel 4: Sichern von Daten 91

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

Einführung

CA ARCserve Backup ist eine umfassende Sicherungslösung für Anwendungen, Datenbanken, verteilte Server und Dateisysteme. Sie bietet Sicherungs- und Wiederherstellungsfunktionen für Datenbanken, unternehmenswichtige Anwendungen und Netzwerk-Clients.

CA ARCserve Backup enthält verschiedene Agenten, unter anderem den CA ARCserve Backup Agent für virtuelle Rechner. Mit dem Agent können Sie virtuelle Rechner (VMs, Virtual Machines) schützen, auf denen folgende Systeme ausgeführt werden:

- **VMware ESX/ESXi Server und VMware vCenter Server--**VMware stellt die Mechanismen VMware Consolidated Backup (VCB) und Virtual Disk Development Kit (VDDK) bereit, die in VMware ESX/ESXi Server und VMware vCenter Server integriert sind. VCB und VDDK ermöglichen den Schutz von VM-Dateien und -Daten (Virtual Machine, engl. für: Virtueller Rechner). Mit VCB oder VDDK können Sie VM-Sicherungsaktivitäten auf ein dafür vorgesehenes Sicherungs-Proxy-System übertragen und anschließend die virtuellen Rechner mit den Sicherungs- und Wiederherstellungsfunktionen von CA ARCserve Backup schützen.
- **VMware vSphere--**VMware vSphere ist ein Virtualisierungswerkzeug, mit dem Sie die aktuellsten Versionen von VMware vCenter Server, VMware VCB und VMware VDDK in CA ARCserve Backup integrieren können.
- **Microsoft Hyper-V:** Microsoft Hyper-V ist eine im Betriebssystem Windows Server 2008 enthaltene Komponente. Hyper-V ist eine Technologie, die auf Hypervisor basiert und es Ihnen ermöglicht, mehrere Betriebssysteme unabhängig von Windows Server 2008 auszuführen. Mit CA ARCserve Backup können Sie Daten auf den Gastbetriebssystemen und auf dem Betriebssystem Windows Server 2008 sichern und wiederherstellen.

So schützt der Agent VMware-Systeme mithilfe von VCB

Der Agent ermöglicht Ihnen die Datensicherung und funktioniert unter den folgenden Umständen besonders gut:

- Sie möchten die Einschränkung von Ressourcen im VMware ESX-Hostsystem reduzieren.

  Hinweis: VMware ESX/ESXi ist eine Anwendung zur Verwaltung von System-, Speicher- und Netzwerkressourcen in mehreren VM-Umgebungen.

- Ihre Umgebung besteht aus VMs, die sich in verschiedenen Datenspeichern befinden.
- Sie möchten Daten auf Datei- oder Raw-Ebene (vollständige VM) wiederherstellen.

Mit VCB können Sie folgende Aufgaben ausführen:

- Einen Snapshot eines virtuellen Rechners erstellen und die Sicherungsdaten in ein oder mehrere Sicherungs-Proxy-Systeme laden oder exportieren und die Ladung vom VMware ESX-Hostsystem entfernen.
- Sicherungen auf Dateiebene und Wiederherstellungen einer VM durchführen, auf der ein von VMware unterstütztes Windows-basiertes Betriebssystem ausgeführt wird.
- Sicherungen auf Raw-Ebene (vollständige VM) und Wiederherstellungen einer VM mit einem beliebigen von VMware unterstützten Betriebssystem durchführen.
- LAN (Local Area Network)-freie Sicherungen durchführen, sofern sich die VMs in einem SAN befinden.
- Eine VM unabhängig von ihrem Status sichern.
- Verwaltungsaufwand durch zentrale Sicherungsverwaltung auf Sicherungs-Proxysystemen reduzieren. Sie müssen keine Agenten auf den VMs verwenden.

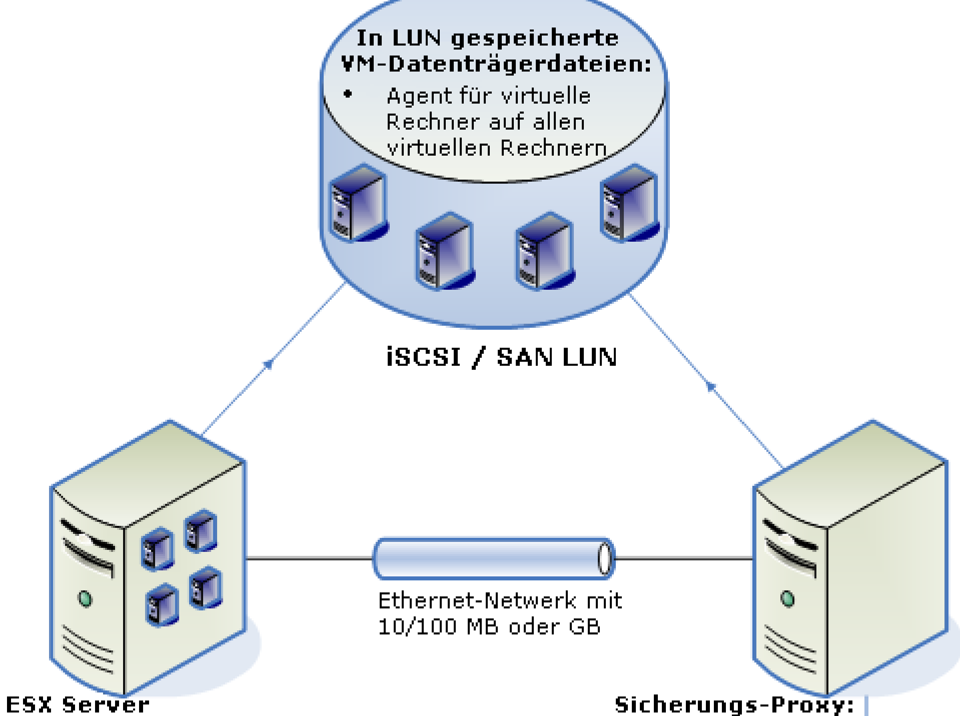
  Hinweis: Diese Funktion erfordert die Installation des Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

Einsatz von VCB durch CA ARCserve Backup zum Schutz Ihrer VMware-Umgebung

Mit diesem Agenten können Sie VM-Sicherungen auf Raw-Ebene (vollständige VM), VM-Sicherungen auf Dateiebene und VM-Sicherungen im gemischten Modus unter Verwendung eines Sicherungs-Proxysystems durchführen.

Die folgende Abbildung veranschaulicht die Netzwerkarchitektur zur Sicherung von VMware-Images oder -Dateien mithilfe eines Sicherungs-Proxysystems:

Sichern einer VMware-Umgebung über ein externes Sicherungs-Proxy-System mit CA ARCserve Backup Agent für virtuelle Rechner



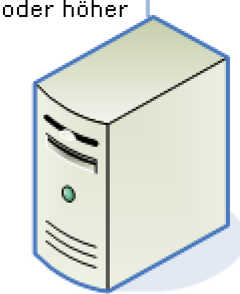
ESX Server

- Auf iSCSI/SAN LUN befindliche virtuelle Rechner
- Auf lokalem Speicher befindliche VM-Datenträgerdateien

Sicherungs-Proxy:

- VMware VCB-Framework/ VDDK
- Agent für virtuelle Rechner
- Client Agent für Windows
- Microsoft .Net-Framework 2.0 oder höher

Wichtig! Die SAN/iSCSI LUNS, die die virtuellen Rechner enthalten, müssen für das Sicherungs-Proxy-System und das ESX/ESXi Server-System zugreifbar sein.



Hinweis: Der Agent unterstützt das Sichern und Wiederherstellen lokal konfigurierter virtueller Rechner auf dem ESX/ESXi Server-System.

Sicherungsserver:

- CA ARCserve Backup-Server

1. Der CA ARCserve Backup-Primärserver oder -Mitgliedsserver kommuniziert mit dem Agenten für virtuelle Rechner, der während der Ausführung des Sicherungsjobs auf dem Sicherungs-Proxysystem ausgeführt wird. Der Agent erstellt dann einen Snapshot des virtuellen Rechners und lädt oder exportiert diesen standardmäßig in das Installationsverzeichnis des Client Agent für Windows auf dem Sicherungs-Proxy-System.
2. Falls beim Sicherungsmodus die Option "Wiederherstellung im Dateimodus erlauben (siehe Seite 95)" angegeben ist, erstellt CA ARCserve Backup Katalogdateien für die Volumes auf dem virtuellen Rechner.
3. Anschließend werden der virtuelle Rechner und die Kataloge auf den Zieldatenträgern gesichert.

Hinweis: Informationen zum Ändern des Standardbereitstellungspfades finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

Wenn Sie diese Architektur in Ihrer Umgebung verwenden, berücksichtigen Sie Folgendes:

- Der Agent muss auf dem Primärserver bzw. auf dem eigenständigen Server von CA ARCserve Backup lizenziert sein.
- Der Agent muss auf allen virtuellen Rechnern installiert sein, auf denen Sie Wiederherstellungen auf Dateiebene für das Gastbetriebssystem durchführen möchten.

  Hinweis: Weitere Informationen finden Sie unter "Installationsorte für den Agenten" (siehe Seite 34).
- Auf dem Sicherungs-Proxysystem muss Microsoft .NET Framework Version 2.0 oder höher ausgeführt werden.
- Wenn sich der virtuelle Rechner auf einer SAN LUN befindet, muss die LUN zwischen dem VMware ESX Host- und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

  Hinweis: Die obige Einschränkung gilt nur für die VCB-Versionen 1.0, 1.0.1 und 1.0.2. Bei VCB ab Version 1.0.3 ist keine einheitliche LUN-Nummer erforderlich.

  Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

  Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware VCB-Dokumentation.
- Die Sicherung auf Raw-Ebene (vollständige VM) erstellt eine Kopie der gesamten Festplatte und aller Konfigurationsdateien, die zu einer bestimmten VM gehören. Damit wird Ihnen die Wiederherstellung der gesamten VM ermöglicht.

  Die Sicherung auf Raw-Ebene kann zur Wiederherstellung von VMs im Falle eines Systemausfalls oder totalen Verlusts der ursprünglichen virtuellen Rechner verwendet werden.
- Mithilfe der Sicherung auf Dateiebene können Sie eine Kopie einzelner Dateien auf der Festplatte einer VM erstellen. Dies kann alle Dateien umfassen.

  Sie können diese Methode in Situationen verwenden, in denen beschädigte oder versehentlich gelöschte Dateien wiederhergestellt werden.

- Bei Sicherungen im gemischten Modus können Sie GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen.

  Sie können mit dieser Methode Daten mit der Effizienz des Raw-Modus sichern (vollständige VM) und mit Dateiebenengranularität wiederherstellen.

- Wenn Sie einen Sicherungsjob übergeben, können Sie eine Sicherung auf Raw-Ebene (vollständige VM) oder Dateiebene der VM durchführen. Sie müssen den Primär- oder Mitgliedsserver angeben, auf dem der Job ausgeführt wird.

  Wichtig! Zur Durchführung von VM-Sicherungen auf Dateiebene muss ein von VMware unterstütztes Windows-Betriebssystem auf der VM installiert sein.

So schützt der Agent VMs in einem lokalen Speicher und einem SAN

Mit dem CA ARCserve Backup Agent für virtuelle Rechner können Sie VMware-basierte Daten schützen, die sich an einem lokalen Speicherort oder in einem Storage Area Network (SAN) befinden. Für alle Datenspeichertypen müssen VMs über das Sicherungs-Proxysystem zugänglich sein.

Die folgende Liste beschreibt die Umgebungskonfiguration, die für jeden Datenspeichertyp erforderlich ist:

- **SAN-, iSCSI-Datenspeicher:** Das Sicherungs-Proxysystem muss über dieselbe SAN- bzw. iSCSI-Infrastruktur mit dem Laufwerk des VMs verbunden sein.
- **Datenspeicher des lokalen Speichers:** Die VMs müssen sich auf Laufwerken befinden, die direkt mit dem VMware ESX-Hostsystem verbunden sind. In Umgebungen mit lokalem Speicher sollte das Sicherungs-Proxy-System über das LAN mit dem VMware ESX-Hostsystem kommunizieren können.

Hinweis: Die Begriffe SAN und iSCSI weisen auf einen gemeinsamen Speicher zwischen Proxy-Systemen und VMware ESX-Hostsystemen hin. Der Begriff SAN gilt auch für iSCSI-Umgebungen, in denen Festplatten mittels iSCSI-Infrastruktur freigegeben werden.

Wenn Sie den Agent in VI 2.5 implementieren und mithilfe des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" oder des ARCserve VMware-Konfigurationstools Informationen in die CA ARCserve Backup-Datenbank füllen, kann CA ARCserve Backup den Agent so konfigurieren, dass er die Datenspeichertypen der VMs in Ihrem Netzwerk erkennt.

Wenn sich die VMs auf einem SAN befinden und das Sicherungs-Proxy-System nicht mit demselben SAN verbunden ist, versucht CA ARCserve Backup, die VMs zu sichern, indem die Informationen verwendet werden, die in der folgenden Datei auf dem Sicherungs-Proxy-System enthalten sind:

```
C:\Programme\CA\ARCserve Backup Client Agent für Windows\VMDatastoreTypes
```

Wenn CA ARCserve Backup die erforderlichen Informationen über die VMs nicht mithilfe der VMDatastoreTypes.ini-Datei sichern kann, fährt CA ARCserve Backup mit der Sicherung unter Verwendung der NBD-Kommunikation (Network Block Device) fort.

Einschränkungen für VCB

Wenn Sie VCB in Ihrer Umgebung verwenden, sollten Sie die folgenden Einschränkungen bedenken:

- Sie können keine VMs mit virtuellen Festplatten sichern, bei denen es sich um kompatible Raw Device Maps (RDM) mit der Eigenschaft "Unabhängig (Persistent/Nicht persistent)" handelt.
- Sie müssen allen Volumes einer VM, die Sie sichern möchten, einen Laufwerksbuchstaben zuweisen und über die Funktion zum Durchsuchen des Ladeverzeichnisses verfügen. Wird dem Volume kein Laufwerksbuchstabe zugeordnet, verhindert VCB, dass Sie das geladene Volume im Ladeverzeichnis suchen können. Dies führt dazu, dass CA ARCserve Backup die Sicherung nicht abschließen kann und den Job als unvollständig ausweist.
- Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

  Hinweis: Die obige Einschränkung gilt nur für die VCB-Versionen 1.0, 1.0.1 und 1.0.2. Bei VCB ab Version 1.0.3 ist keine einheitliche LUN-Nummer erforderlich.

  Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

  Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware VCB-Dokumentation.

- Um eine einzelne Datei oder ein einzelnes Verzeichnis zu sichern, muss ein von VMware unterstütztes Windows-basiertes Betriebssystem auf der VM laufen.
- VCB unterstützt Ladungen mit bis zu 60 gleichzeitigen VM-Volumes.

Beispiele: Laden von gleichzeitigen VMware Volumes

  - 60 VMs mit einem C:\ Laufwerk
  - 30 VMs mit zwei VM-Volumes: einem C:\ Laufwerk und einem D:\ Laufwerk

- VCB unterstützt die Verwendung nicht englischer Multibyte-Zeichen nicht. Pfade und Registrierungszeichenfolgen mit nicht englischen Multibyte-Zeichen werden möglicherweise nicht richtig angezeigt.

Hinweis: Informationen zur Installation und zum Setup von VCB sowie zu den Einschränkungen bei der Verwendung von VCB finden Sie im Handbuch "VMware Virtual Machine Backup Guide" auf der Website von VMware.

Schutz durch den Agenten von VMware vSphere-Systemen mithilfe von VDDK

CA ARCserve Backup ermöglicht den Schutz von VMware vSphere-Systemen unter Verwendung von VDDK.

Dieser Abschnitt enthält folgende Themen:

Installation von VMware VDDK auf den Installationsdatenträgern

CA ARCserve Backup installiert VMware Virtual Disk Development Kit (VDDK) 1.2.1 auf allen Systemen, auf denen Sie den Agenten installieren. Sie müssen VDDK nicht herunterladen und auf Ihren Sicherungs-Proxy-Systemen installieren.

Einführung zur Integration in VMware vSphere

CA ARCserve Backup Agent für virtuelle Rechner ist in die aktuellste Version von VMware Virtual Infrastructure namens vSphere integriert. Mit dieser Funktionalität können Sie virtuelle Rechner (VMs) in vSphere-Umgebungen schützen (die VMs befinden sich z. B. in ESX Server 4.0-Systemen und vCenter Server 4.0-Systemen). Der Agent erleichtert den Schutz von VMs mithilfe von VMware Virtual Consolidated Backup Framework (VCB) 1.5 Update 1 oder höher und VMware Virtual Disk Development Kit (VDDK) 1.1 oder höher.

VDDK ermöglicht Ihnen den Remote-Zugriff auf VM-Festplatten auf ESX Server-Systemen, ohne dass Sie die Festplatten zum Sicherungs-Proxy-System exportieren müssen. Die Integration in VDDK stellt Ihnen eine alternative Vorgehensweise für die Verwendung von VCB Framework zur Sicherung virtueller Rechner. Diese Vorgehensweise kann nur auf den Systemen ESX Server 4.0, ESX Server 3.5, vCenter 4.0 und VirtualCenter Server 2.5 verwendet werden.

VMware Virtual Disk Development Kit (VDDK) ist eine Gruppe von APIs und Verwaltungstools, mit denen Sie virtuelle Speichersysteme erstellen, verwalten und auf diese zugreifen können. VMware VDDK wird auf Version x86 und x64 von Windows und auf Linux-Betriebssystemen unterstützt.

Die Verwendung eines VDDK bietet folgende wesentliche Vorteile:

- Mit VDDK ist es nicht mehr erforderlich, VM-Snapshots auf dem Sicherungs-Proxy-System zu speichern. Bei Verwendung von VDDK kann CA ARCserve Backup Daten für alle Raw-Sicherungen (vollständige VM) direkt von den ESX Server-Datenspeichern zum Sicherungsdatenträger übertragen.

  Hinweis: Bei der Bearbeitung von Raw-Sicherungen (vollständige VM) mit Auswahl der Option "Wiederherstellung auf Dateiebene erlauben" speichert CA ARCserve Backup die Sektoren entsprechend den Festplatten- und Dateisystem-Metadaten auf dem Sicherungs-Proxy-System.

- VDDK minimiert die Abhängigkeit von VMware-Tools. Bei Verwendung von VDDK ist es für CA ARCserve Backup nicht erforderlich, dass auf den Sicherungs-Proxy-Systemen VMware Virtual Consolidated Backup (VCB) installiert ist. Des Weiteren wird zur Wiederherstellung von VMs nicht der VMware Converter benötigt. VDDK bietet weitere Steuerungsfunktionen und verbesserte Berichtsfunktionen zur Sicherung und Wiederherstellung von VMs.

Hinweis: Die aktuellste ESX Server-Version ist VMware vSphere 4.0 Update 1. Die neueste Version von VMware vCenter Server ist VMware vCenter Server 4.0 Update 1.

Es gibt zwei Vorgehensweisen, die Sie verwenden können, um Ihre VM-Umgebung zu schützen:

- Über das ESX Server- oder ESXi Server-Host-System: Ein einzelner Host kann nur die VMs verwalten, die sich innerhalb des Hostsystems befinden. Diese Methode verwendet VCB Framework und VDDK zur Durchführung von Sicherungen und Wiederherstellungen.
- Über das vCenter Server-System: Ein vCenter Server-System kann VMs verwalten, die über viele ESX Server- und ESXi Server-Host-Systeme verteilt sind. Diese Methode verwendet VCB Framework und VDDK zur Durchführung von Sicherungen und Wiederherstellungen.

So verwenden Sie den Agent mit VMware vSphere

Die Verwendung von VMware vSphere kann sich darauf auswirken, wie Sie Ihre Sicherungsinfrastruktur planen.

Ohne VMware vSphere wird CA ARCserve Backup in VMware Virtual Infrastructure (Version 2.0 und 2.5) mithilfe der VMware VCB Framework-Tools zum Sichern von VM-Daten integriert. Bei der Verwendung von VCB Framework müssen Sie einen Windows-Server als Sicherungs-Proxy-System festlegen. Das Sicherungs-Proxy-System benötigt zum Staging der Snapshot-Aufnahmen von den gesicherten VMs viel freien Festplattenspeicher.

Um eine vollständige VM wiederherzustellen (beispielsweise zur Wiederherstellung einer VM nach einem Systemausfall), muss auf dem Sicherungs-Proxy-System der VMware Converter installiert sein. VMware bietet verschiedene Konvertierungstools an. Allerdings unterstützt CA ARCserve Backup nur die Verwendung unabhängiger Versionen von Konvertierungstools.

Hinweis: CA ARCserve Backup kann zur Wiederherstellung von VMs keine Unternehmensversionen von VMware Converter verwenden.

Bei der Integration in VMware vSphere werden die folgenden Vorgänge durchgeführt:

- Sichern von VMs auf allen derzeit unterstützten Versionen von VMware ESX Server und VMware VirtualCenter Server mithilfe von VMware VCB-Framework.

- Sichern Sie VMs, die sich auf ESX Server 4.0-Systemen oder anderen Hosts befinden, die von Center Server 4.0 unter Verwendung von VDDK verwaltet werden.
- Sichern Sie VMs, die sich auf ESX Server 4.0-Systemen oder anderen Hosts befinden, die von Center 4.0 unter Verwendung von VCB Framework 1.5 Update 1 verwaltet werden.
- Sichern und stellen Sie VMs, die sich in den folgenden Umgebungen befinden, unter Verwendung einer neuen Vorgehensweise wieder her:
  - ESX Server-Systeme, Version 4.0 und höher
  - VirtualCenter Server-Systeme, Version 4.0 und höher

  Bei dieser neuen Methode, die von VMware empfohlen wird, können Sie eine Kombination aus den APIs, die von VMware vSphere Web Service SDK bereitgestellt werden, und VMware VDDK verwenden.

Beispiele: So verwenden Sie den Agent mit VMware vSphere

- Geringere Hardware-Voraussetzungen: Zum Sichern und Wiederherstellen von VMs wird kein Sicherungs-Proxy-System benötigt. Sie können VMs vom Primärserver oder einem Mitgliedsserver aus sichern und wiederherstellen, ohne dass es zu einer zusätzlichen Belastung des CA ARCserve Backup-Servers kommt.
- Kein temporärer Ladeort mehr erforderlich: Zur Sicherung von VMs in einer VMware-Sicherungsumgebung mithilfe der VCB-Tools wird auf dem Sicherungs-Proxy-System ein Ladeort mit einem großen verfügbaren Festplattenspeicher benötigt. Wenn Sie Raw-Sicherungen (vollständige VM) mit Auswahl der Option "Wiederherstellung im Dateimodus erlauben" durchführen, muss die Menge an freiem Festplattenspeicher auf dem Sicherungs-Proxy-System der Gesamtgröße aller VMs entsprechen, die Sie mithilfe von Multistreaming gleichzeitig sichern können. Bei der neuen Methode muss CA ARCserve Backup die VM-Sicherungen nicht mehr auf dem Sicherungs-Proxy-System speichern. Folglich ermöglicht es Ihnen dieser Agent, auf dem Sicherungs-Proxy-System Systemressourcen und Festplattenspeicher freizugeben.

- Geringere Softwareabhängigkeit: Sie müssen auf dem Sicherungs-Proxy-System weder VCB noch VMware Converter installieren. Dadurch werden auf dem Sicherungs-Proxy-System Systemressourcen und Festplattenspeicher freigegeben. Die Verwendung des Agent mit vSphere VMware erfordert weniger Software zum Verwalten Ihrer VM-Sicherungen und -Wiederherstellungen. Wenn Sie die neue Methode mit VMware vSphere Web Services SDK und VDDK verwenden, installieren Sie auf dem Sicherungs-Proxy-System zur Durchführung von Sicherungen und Wiederherstellungen nur VDDK. Dadurch werden die VM-Berichtfunktionen verbessert und die Verwaltung Ihrer VMs vereinfacht, da weniger Komponenten vorhanden sind, die ausfallen können.

So wird vSphere in früheren Agent-Versionen integriert

Zusätzlich zu dem von dieser Agent-Version bereitgestellten Schutz können Sie die folgenden Vorgänge durchführen:

- Sichern von Daten auf Dateiebene und Raw-Daten (vollständige VM-Sicherung) mithilfe von CA ARCserve Backup r12.5 mit VMware VDDK in einer Umgebung, in der eine ältere Version von ESX Server oder VirtualCenter Server ausgeführt wird.
- Stellen Sie Raw-Daten (vollständiger VMs) und Daten auf Dateiebene via Restore wieder her, und führen für VMs eine Recovery mithilfe von Daten durch, die mit CA ARCserve Backup r12, CA ARCserve Backup r12 SP1, CA ARCserve Backup r12 SP2, CA ARCserve Backup r12.5, CA ARCserve Backup r12.5 SP1, CA ARCserve Backup r15 oder CA ARCserve Backup r15 SP1 unter Verwendung von VDDK gesichert wurden.

Hinweis: Informationen über die Aufgaben, die Sie mit vSphere ausführen können, finden Sie unter Aufgaben, die Sie mit dem vSphere-Patch ausführen können.

Schutz von Hyper-V-Systemen durch den Agenten

Der Agent ermöglicht Ihnen das Sichern von Daten und funktioniert am besten, wenn Sie Daten auf Dateiebene, Raw-Ebene (vollständige VM) oder auf gemischter Ebene wiederherstellen möchten.

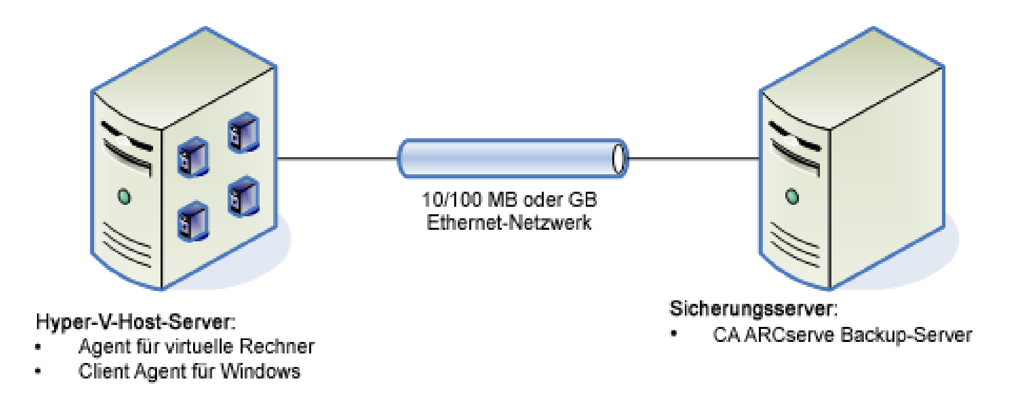
Mit Microsoft Hyper-V können Sie folgende Verwaltungsaufgaben durchführen:

- Sicherungen auf Dateiebene durchführen und auf einer VM mit einem von Hyper-V unterstützten Windows-basierten Betriebssystem wiederherstellen.
- Sicherungen auf Raw-Ebene (vollständige VM) und Wiederherstellungen auf einer VM mit einem beliebigen von Hyper-V unterstützten Betriebssystem durchführen.
- Eine VM unabhängig von ihrem Status sichern.
- Verwaltungsaufwand durch zentrale Sicherungsverwaltung auf Hyper-V-Hostsystemen reduzieren.

Einsatz von Hyper-V durch CA ARCserve Backup zum Schutz Ihrer Umgebung

Mit diesem Agenten können Sie VM-Sicherungen auf Raw-Ebene (vollständige VM), VM-Sicherungen auf Dateiebene und VM-Sicherungen im gemischten Modus durchführen.

Die folgende Abbildung veranschaulicht die Netzwerkarchitektur zur Sicherung von VM-Images oder -Dateien.



Wenn Sie diese Architektur in Ihrer Umgebung verwenden, berücksichtigen Sie Folgendes:

- Der Agent muss auf dem Primärserver bzw. auf dem eigenständigen Server von CA ARCserve Backup lizenziert sein.
- Der Agent muss auf allen virtuellen Rechnern installiert sein, auf denen Sie Wiederherstellungen auf Dateiebene für das Gastbetriebssystem durchführen möchten.

  Hinweis: Weitere Informationen finden Sie unter "Installationsorte für den Agenten" (siehe Seite 34).
- Die Sicherung auf Raw-Ebene (vollständige VM) erstellt eine Kopie der gesamten Festplatte und aller Konfigurationsdateien, die zu einer bestimmten VM gehören. Damit wird Ihnen die Wiederherstellung der gesamten VM ermöglicht.

  Die Sicherung auf Raw-Ebene kann zur Wiederherstellung von VMs im Falle eines Systemausfalls oder totalen Verlusts der ursprünglichen virtuellen Rechner verwendet werden.

- Mithilfe der Sicherung auf Dateiebene können Sie eine Kopie einzelner Dateien auf der Festplatte einer VM erstellen. Dies kann alle Dateien umfassen.

  Sie können diese Methode in Situationen verwenden, in denen beschädigte oder versehentlich gelöschte Dateien wiederhergestellt werden.

- Wenn Sie einen Sicherungsjob übergeben, können Sie eine Sicherung auf Raw-Ebene (vollständige VM) oder Dateiebene der VM durchführen. Sie müssen den Primär- oder Mitgliedsserver angeben, auf dem der Job ausgeführt wird.

  Wichtig! Zur Durchführung von VM-Sicherungen auf Dateiebene muss ein von Hyper-V unterstütztes Windows-Betriebssystem auf der VM installiert sein.

Unterstützte Funktionen

Der Agent unterstützt die folgenden Funktionen:

- **Multistreaming**: Mit CA ARCserve Backup können Sie mithilfe von Multistreaming auf VM-Ebene Jobs übergeben.
- **Staging**: Mit CA ARCserve Backup können Sie VM-Sicherungsjobs an Disk-Staging- und Band-Staging-Geräte übergeben.

  Sie können Daten auf Dateiebenengranularität direkt vom Staging-Gerät und von einem endgültigen Zieldatenträger, wie zum Beispiel einem Banddatenträger, wiederherstellen.

- **Deduplizierung**: Mit CA ARCserve Backup können Sie Speicherplatz sparen, indem Sie Blöcke redundanter Sicherungsdaten löschen.

- **Multiplexing**: Mit CA ARCserve Backup können Sie Jobs mithilfe von Multiplexing übergeben.
- **GFS- und Rotationssicherungen**: Mit CA ARCserve Backup können Sie GFS- und Rotationssicherungsjobs übergeben.
- **Ergänzungsjobs:**
  - **Raw-(vollständige VM-)Sicherungen**: CA ARCserve Backup startet den fehlgeschlagenen Job auf VM-Ebene neu.
  - **Zuwachs- und Änderungssicherungen**: CA ARCserve Backup startet fehlgeschlagene Jobs auf Volume-Ebene neu.
- **Komprimierung**: Mit CA ARCserve Backup können Sie VM-Sicherungsdaten auf dem Agent-System oder dem CA ARCserve Backup-Server komprimieren.
- **Verschlüsselung**: Mit CA ARCserve Backup können Sie VM-Sicherungsdaten auf dem Agent-System oder dem CA ARCserve Backup-Server verschlüsseln.
- **CRC-Prüfung**: Da die CRC-Prüfung auf VM-Sicherungsdaten unterstützt wird, haben Sie mit CA ARCserve Backup die Möglichkeit, die Datenintegrität zu überprüfen.
- **Übergreifende und gespiegelte RAID-5-Volumes und RAID-5-Stripesetvolumes**: Mit CA ARCserve Backup können Sie VM-Daten auf übergreifenden und gespiegelten RAID-5-Volumes und RAID-5-Stripesetvolumes schützen.
- **Partitionsgerätzuordnung (Raw Device Mapping, RDM)**: Mit CA ARCserve Backupkönnen Sie Daten auf Volumes sichern, auf denen Raw Device Mapping (RDM) im virtuellen Kompatibilitätsmodus konfiguriert ist. CA ARCserve Backup unterstützt diese Funktion bei VCB- und VDDK-basierten Sicherungen.

  Wenn Sie Daten mithilfe der Methode "Virtuellen Rechner wiederherstellen" wiederherstellen, werden RDMs, die im virtuellem Kompatibilitätsmodus konfiguriert sind, als normale virtuelle Datenträger wiederhergestellt.
- **Dynamischer Speicher für Hyper-V**: Windows Server 2008 R2 SP1 unterstützt die Möglichkeit, verfügbaren Speicher für virtuelle Rechner unter Hyper-V anzupassen, wenn sich die Auslastung auf den virtuellen Rechnern ändert. Zur Unterstützung dieser Funktion können Sie mit CA ARCserve Backup VMs wiederherstellen, die mit dynamischem Speicher für Hyper-V gesichert wurden, für den der verfügbare Speicher, der ursprünglich den VMs zugewiesen wurde, angegeben wurde.

Agent-Analyse von Daten, die sich auf virtuellen Rechnern befinden

Virtuelle Rechner (VMs), auf denen VMware vSphere und Microsoft Hyper-V ausgeführt werden, können die verwendeten Datenblöcke auf virtuellen Datenträgern identifizieren. Mit dieser Funktion wird die allgemeine Sicherungsdauer für Jobs in CA ARCserve Backup vermindert. Die umfassende Sicherungsdauer verringert sich, da CA ARCserve Backup nur die verwendeten Datenblöcke sichert und nicht den ganzen Datenträger.

CA ARCserve Backup verwendet den Ansatz der Blockanalyse, wenn Daten gesichert werden, die sich auf Hyper-V-VMs befinden oder auf VMware-VMs, in deren Umgebung VMware vSphere Webservices SDK und VMware VDDK ausgeführt werden. Außerdem muss Verfolgung der Blockänderung auf den VMware-VMs aktiviert werden. Weitere Informationen zur Verfolgung der Blockänderung finden Sie auf der VMware-Website.

Hinweis: In VMware-VMs müssen Sie eine Sicherungsvorgehensweise angeben. Weitere Informationen dazu finden Sie unter Festlegen von Sicherungsmethoden (siehe Seite 51).

Bei der Sicherung von virtuellen Rechnern sichert CA ARCserve Backup nur aktive Blöcke der Phase der vollständigen Sicherung bei Raw-Sicherungen (vollständiger virtueller Rechner), ohne oder mit aktivierter Option "Wiederherstellung auf Dateiebene zulassen", sowie gemischter Sicherungen mit aktivierter Option "Wiederherstellung auf Dateiebene zulassen".

Beachten Sie Folgendes:

- Bei Hyper-V-VMs verwendet CA ARCserve Backup die Vorgehensweise der aktiven Blockanalyse nicht für Sicherungen, wenn der Agent keine Datenträger-Bitmaps des virtuellen Rechners erstellen kann. Der Agent kann Datenträger-Bitmaps nicht erstellen, wenn die übergeordnete virtuelle Festplatte (VHD) ein eingebauter Datenträger und kein Datenträger mit dynamischer Erweiterung ist. Wenn der Agent diese Bedingung erkennt, kehrt CA ARCserve Backup zum früheren Sicherungsverhalten zurück, bei dem jeder Datenblock innerhalb der Sicherung analysiert wird.

Einschränkungen beim Sichern und Wiederherstellen auf virtuellen Rechnern

Die folgenden Einschränkungen gelten für die Sicherung und Wiederherstellung auf virtuellen Rechnern:

- Die VMs im VMware ESX-Hostsystem müssen ausgeführt werden, während Sie die CA ARCserve Backup-Datenbank auffüllen.

  Die virtuellen Rechner müssen ausgeführt werden, damit die CA ARCserve Backup-Datenbank von den Konfigurationstools ARCserve VMware (ca_vcbpopulatedb.exe) und ARCserve Hyper-V (ca_msvmpopulatedb.exe) mit den korrekten Daten gefüllt werden kann und damit die virtuellen Rechner in VMware ESX-Hostsystemen richtig durchsucht werden können.

- Sie müssen das ARCserve VMware-Konfigurationstool (ca_vcbpopulatedb.exe) und das ARCserve Hyper-V-Konfigurationstool (ca_msvmpopulatedb.exe) ausführen, nachdem Sie Volumes auf einem virtuellen Rechner bzw. einen virtuellen Rechner in einem Hostsystem hinzugefügt, entfernt oder geändert haben.

  Ein Versäumnis dessen kann zu inkorrekten VM-Volume-Daten in der CA ARCserve Backup-Datenbank führen, und während der Laufzeit kommt es dann zu fehlgeschlagenen Sicherungsjobs.

- In CA ARCserve Backup kann die Befehlszeile nicht für Sicherungen und Wiederherstellungen auf virtuellen Rechnern verwendet werden. Z. B. ca_backup und ca_restore.

  Sie müssen für alle VM-basierten Sicherungen und Wiederherstellungen den Sicherungs-Manager und den Wiederherstellungs-Manager verwenden.

- Sie können die Methode "Wiederherstellung nach Datenträger" nicht zur Wiederherstellung von Sicherungsdaten auf Dateiebene und Raw-Ebene (vollständige VM) verwenden.

- Das Hilfsprogramm "Vergleichen" unterstützt keine Vergleiche von VM-Sicherungssitzungen.

  Wenn Sie versuchen, VM-Sitzungen zu vergleichen, führt CA ARCserve Backup anstelle des Vergleichs einen Suchvorgang aus.

- Der Agent bietet keine Unterstützung für die folgenden globalen Sicherungsoptionen:
  - Dateien nach Sicherungsjob löschen
  - Wiederholungsverfahren bei Zugriff auf geöffnete Dateien

  Hinweis: Weitere Informationen zu globalen Sicherungsoptionen finden Sie im "*Administrationshandbuch*".

- Aufgrund der Einschränkungen bei den technischen und logischen Zuordnungen von Volumes in der CA ARCserve Backup-Datenbank unterstützt das Hilfsprogramm "Einfügen" kein sequenzielles Einfügen.

  Falls Sie Daten zu VM-Sitzungen in die CA ARCserve Backup-Datenbank einfügen möchten, können Sie die Katalogdaten einfügen.

- Vom Agent unterstützte VM-Bereitstellungspfade dürfen ausschließlich englische Zeichen enthalten. Wenn der Pfad nicht englische Zeichen enthält, werden diese unlesbar angezeigt.

Kapitel 2: Installieren und Konfigurieren des Agenten

Dieses Kapitel enthält folgende Themen:

Lizenzierung des Agenten

Der CA ARCserve Backup Agent für virtuelle Rechner verwendet eine anzahlbasierte Lizenzierungsmethode. Sie müssen für jeden virtuellen Rechner und jedes Hostsystem, das mit CA ARCserve Backup geschützt wird, einen CA ARCserve Backup Agent für virtuelle Rechner lizenzieren. Die Lizenzen für den Agenten müssen auf dem Primärserver oder auf dem eigenständigen Server von CA ARCserve Backup registriert werden.

Beispiele: Lizenzierung des Agenten

Die folgende Liste beschreibt Standardinstallationsszenarien:

- Ihre Umgebung besteht aus einem Hyper-V-Host mit drei Gastbetriebssystemen. Sie müssen vier Lizenzen (1 Hostsystem plus 3 VMs) auf dem CA ARCserve Backup-Server lizenzieren.
- Ihre Umgebung besteht aus einem VMware ESX-Hostsystem mit drei Gastbetriebssystemen. Sie müssen vier Lizenzen (1 Sicherungs-Proxy-System plus 3 VMs) auf dem CA ARCserve Backup-Server lizenzieren.

- Ihre Umgebung besteht aus zwei Hyper-V-Hostsystemen. Jedes Hyper-V-Hostsystem besteht aus drei Gastbetriebssystemen. Sie müssen acht Lizenzen (1 Hostsystem plus 3 VMs, 1 Hostsystem plus 3 VMs) auf dem CA ARCserve Backup-Server registrieren.
- Ihre Umgebung besteht aus einem VM-Hostsystem (VMware ESX Host oder Hyper-V Server) mit zwei VMs. Sie benötigen nur Raw-Sicherungen (vollständige VM) und arbeiten ohne die Option "Wiederherstellung im Dateimodus erlauben". In diesem Szenario wird der Agent nur auf dem Hostsystem installiert. Auf dem CA ARCserve Backup-Server muss jedoch eine Lizenz für jeden virtuellen Rechner registriert werden. Daher müssen Sie drei Lizenzen (1 Hostsystem plus 2 VMs) auf dem CA ARCserve Backup-Server registrieren.

Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter "Funktionsweise des globalen und lokalen Sicherungsmodus (siehe Seite 95)".

Installationsorte für den Agenten

Als eine allgemeine Best Practice müssen Sie den Agent an den folgenden Speicherorten installieren:

- VMware-Umgebungen: auf den Sicherungs-Proxy-Systemen und auf den VMs, die Sie schützen möchten.
- Hyper-V-Umgebungen: auf den Hyper-V-Hostsystemen und auf den VMs, die Sie schützen möchten.

Allerdings entscheidet der Sicherungsmodus, den Sie für Ihre Sicherungen benötigen, wo Sie den Agenten installieren müssen.

Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter "Funktionsweise des globalen und lokalen Sicherungsmodus (siehe Seite 95)".

Die folgende Tabelle gibt an, welchen Typ von Sicherungsmodi Sie benötigen und wo Sie den Agenten installieren müssen.

Ausgewählter Sicherungsmodus	Hyper-V-Hostsystem	VMware-Sicherungs-Proxysystem	Hyper-V-VM	VMware VM
Dateimodus	Benötigt	Benötigt	Benötigt	Nicht benötigt

Ausgewählter Sicherungsmodus	**Hyper-V-Hostsystem**	**VMware-Sicherungs-Proxysystem**	**Hyper-V-VM**	**VMware VM**
Raw-Modus (vollständige VM-Sicherung) *ohne* Auswahl der Option "Wiederherstellung auf Dateiebene erlauben"	Benötigt	Benötigt	Nicht benötigt	Nicht benötigt
Raw-Modus (vollständige VM-Sicherung) *mit* Auswahl der Option "Wiederherstellung auf Dateiebene erlauben"	Benötigt	Benötigt	Benötigt	Benötigt
Gemischter Modus *ohne* Auswahl der Option "Wiederherstellung auf Dateiebene erlauben"	Benötigt	Benötigt	Benötigt	Nicht benötigt
Gemischter Modus *mit* Auswahl der Option "Wiederherstellung auf Dateiebene erlauben"	Benötigt	Benötigt	Benötigt	Benötigt

Beachten Sie Folgendes:

- Für jede VM, die Sie mit CA ARCserve Backup schützen, müssen Sie eine Lizenz registrieren. Alle Lizenzen müssen auf dem Primärserver oder auf dem eigenständigen Server registriert werden.
- Für den Agenten ist der CA ARCserve Backup Client Agent für Windows erforderlich. Sie müssen den Client Agent für Windows an allen Speicherorten installieren, an denen Sie den Agenten für virtuelle Rechner installiert haben.

Sicherungsmodus und Installationsmatrix

Der Sicherungsmodus, der zum Sichern von VM-Daten verwendet werden kann, ist abhängig vom Installationsort des Agenten für virtuelle Rechner. In der folgenden Tabelle finden Sie eine Übersicht über die möglichen Sicherungsmodi mit dem jeweiligen Installationsort des Agenten.

Weitere Informationen zu den Sicherungsmodi finden Sie unter "Funktionsweise des globalen und lokalen Sicherungsmodus (siehe Seite 95)".

VMware-Systeme

Schlüssel:

- Beim **Raw**-Sicherungsmodus handelt es sich um eine Sicherung im Raw-Modus (gesamte VM) mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Beim **gemischten** Sicherungsmodus handelt es sich um eine Sicherung im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Der Begriff **Agent** bezieht sich auf den Agenten für virtuelle Rechner.
- Der Ausdruck **Client Agent** bezieht sich auf den Client Agent für Windows.

  Wichtig! Der Client Agent für Windows ist eine für den Agenten für virtuelle Rechner erforderliche Komponente.

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwenden von VCB/VDDK	**Verwenden des Client Agent**	**Verwenden von VCB/VDDK**	**Verwenden des Client Agent**
Muss der Agent auf dem virtuellen Rechner/Gast-BS installiert werden?	Nein	Nein	Ja	Nein	Ja	Ja	Ja

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwenden von VCB/VDDK	**Verwenden des Client Agent**	**Verwenden von VCB/VDDK**	**Verwenden des Client Agent**
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, ohne dass der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Ja	Nein	Ja	Nein	Siehe **Hinweis 1**.	Nein

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwenden von VCB/VDDK	**Verwenden des Client Agent**	**Verwenden von VCB/VDDK**	**Verwenden des Client Agent**
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Können Sitzungen wiederhergestellt werden, die in diesem Sicherungsmodus gesichert wurden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Nein	Ja	Ja	Ja, siehe **Hinweis 2**.	Ja	Ja	Ja

Frage	Raw	Datei	Raw #	"Mixed" als globale Option		"Mixed #" als globale Option	
				Verwenden von VCB/VDDK	**Verwenden des Client Agent**	**Verwenden von VCB/VDDK**	**Verwenden des Client Agent**
Lassen sich virtuelle Rechner mithilfe von Daten wiederherstellen, die in dem Sicherungsmodus gesichert wurden, bei dem der Agent auf dem virtuellen Rechner/Gastbetriebssystem installiert war (siehe **Hinweis 3**)?	Nein	Nein	Nein	Nein	Nein	Nein	Nein

Hinweis 1: Sicherungen im Raw-Modus und mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" haben am Ende den Status "Abgeschlossen". Zuwachs- und Änderungssicherungen werden erfolgreich beendet.

Hinweis 2: CA ARCserve Backup führt mithilfe des WMware Converter-Tools Vorgänge zur Wiederherstellung der VM durch, wobei das Tool auf dem Sicherungs-Proxy-System installiert ist. Sie müssen nicht den Agenten für virtuelle Rechner oder den Client Agent für Windows auf der VM installieren, um Vorgänge zur Wiederherstellung der VM durchzuführen.

Hyper-V-Systeme

Schlüssel:

- Beim **Raw**-Sicherungsmodus handelt es sich um eine Sicherung im Raw-Modus (gesamte VM) mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Beim **gemischten** Sicherungsmodus handelt es sich um eine Sicherung im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".
- Der Begriff **Agent** bezieht sich auf den Agenten für virtuelle Rechner.
- Der Ausdruck **Client Agent** bezieht sich auf den Client Agent für Windows.

  Wichtig! Der Client Agent für Windows ist eine für den Agenten für virtuelle Rechner erforderliche Komponente.

Frage	Raw	Datei	Raw #	Gemischt	Gemischt #
Muss der Agent auf dem virtuellen Rechner/Gast-BS installiert werden?	Nein	Ja	Ja	Ja	Ja
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, ohne dass der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Nein	Nein	Nein	Nein
Können Sicherungen in diesem Sicherungsmodus durchgeführt werden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Ja	Ja	Ja	Ja	Ja
Können Sitzungen wiederhergestellt werden, die in diesem Sicherungsmodus gesichert wurden, wenn der Agent auf dem virtuellen Rechner/Gast-BS installiert ist?	Nein	Ja	Ja	Siehe **Hinweis 1**.	Ja
Lassen sich virtuelle Rechner mithilfe von Daten wiederherstellen, die in dem Sicherungsmodus gesichert wurden, bei dem der Agent auf dem virtuellen Rechner/Gastbetriebssystem installiert war (siehe **Hinweis 2**)?	Nein	Nein	Nein	Nein	Nein

Hinweis 1: Ja, Sie können Sitzungen wiederherstellen, die im gemischten Modus gesichert wurden. Dies gilt jedoch nur für Zuwachs- und Änderungssicherungen. Sie können Sitzungen, die im gemischten Modus gesichert wurden, jedoch nicht aus der ersten vollständigen Sitzungssicherung wiederherstellen.

Hinweis 2: Sie müssen den Agenten für virtuelle Rechner oder den Client Agent für Windows nicht auf den Hyper-V-VMs installieren. CA ARCserve Backup verwaltet die Wiederherstellung von Hyper-V-VMs, wenn Sie den Agenten für virtuelle Rechner auf dem Hyper-V-Hostsystem installieren.

Best Practices für die Installation und Konfiguration des Agenten für virtuelle Rechner

Folgende Best Practices sind für die Installation des CA ARCserve Backup Agenten für virtuelle Rechner zu empfehlen:

Task	VMware-Systeme	Hyper-V-Systeme
Erforderliche Komponenten	**CA ARCserve Backup** Installieren Sie die CA ARCserve Backup-Serverkomponenten auf dem System, das als Primärserver oder als eigenständiger Server dienen soll. **Agent für virtuelle Rechner** Installieren Sie den Agent auf dem System, das als Sicherungs-Proxysystem dienen soll. Die Best Practice ist, den Sicherungsserver als Sicherungs-Proxysystem zu verwenden. Sollte diese Konfiguration jedoch Ihrer Einschätzung nach Leistungseinbußen für den Server bedeuten, installieren Sie den Agenten auf einem Remote-System, und nutzen Sie ihn als Sicherungs-Proxy-System. **Hinweis:** Sie müssen die Agent-Lizenz auf dem CA ARCserve Backup-Server registrieren. **VMware VCB Framework/VDDK** Stellen Sie sicher, dass VMware VCB Framework oder VDDK auf dem Sicherungs-Proxy-System installiert ist. **Hinweis:** Als Best Practice sollten Sie VCB Framework und VDDK auf dem Sicherungs-Proxy-System installieren. Diese Konfiguration ermöglicht vollständige VM-Sicherungen und -Wiederherstellungen mithilfe von VDDK sowie Sicherungen im Dateimodus mithilfe von VCB Framework.	**CA ARCserve Backup** Installieren Sie die CA ARCserve Backup-Serverkomponenten auf dem System, das als Primärserver oder als eigenständiger Server dienen soll. **Agent für virtuelle Rechner** Installieren Sie den Agent auf dem Hyper-V-Hostsystem. **Hinweis:** Sie müssen die Agent-Lizenz auf dem CA ARCserve Backup-Server registrieren.

Für das Konfigurieren des CA ARCserve Backup Agenten für virtuelle Rechner und zum Sichern von Daten empfehlen sich folgende Best Practices:

Task	VMware-Systeme	Hyper-V-Systeme
Konfiguration	Füllen Sie mit dem ARCserve VMware-Konfigurationstool auf dem Sicherungs-Proxysystem die CA ARCserve Backup-Datenbank mit Daten. Weitere Informationen finden Sie unter Einpflegen von Informationen in die Datenbank mithilfe des ARCserve VMware-Konfigurationstools (siehe Seite 73). Stellen Sie den Agent für virtuelle Rechner unter Verwendung der Agent-Bereitstellung bereit. Weitere Informationen finden Sie unter Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung (siehe Seite 46).	Befüllen Sie mit dem ARCserve Hyper-V-Konfigurationstool auf dem Hyper-V-Host die CA ARCserve Backup-Datenbank mit Daten. Weitere Informationen finden Sie unter Einpflegen von Informationen in die Datenbank mithilfe des ARCserve Hyper-V-Konfigurationstools (siehe Seite 82). Stellen Sie den Agent für virtuelle Rechner unter Verwendung der Agent-Bereitstellung bereit. Weitere Informationen finden Sie unter Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung (siehe Seite 46).
Sicherungsmodus	Akzeptieren Sie den Standard-Sicherungsmodus, der folgende festgelegte Optionen umfasst: ▪ Sicherung im gemischten Modus ▪ Wiederherstellung auf Dateiebene aktivieren	
Sicherungsoptionen – Multistreaming	Für eine effiziente Durchführung von Sicherungsjobs sollten Sie die Multistreaming-Option verwenden und maximal vier VMs für einen Sicherungsjob angeben. Informationen über Multistreaming finden Sie im *Administrationshandbuch.*	
Sichern von Daten	Folgen Sie den unter Sichern von Daten (siehe Seite 91) beschriebenen Schritten.	

Voraussetzungen für die Installation

Vor der Installation des Agenten müssen Sie zunächst folgende vorbereitende Aufgaben ausführen:

- Stellen Sie sicher, dass das System die für die Installation des Agenten erforderlichen Mindestvoraussetzungen erfüllt.

  Eine Liste der Voraussetzungen finden Sie in der Infodatei.

- Stellen Sie sicher, dass Sie über ein Administratorprofil oder ein Profil mit Rechten für die Softwareinstallation verfügen.
- Stellen Sie sicher, dass Sie den Benutzernamen und das Kennwort des Systems kennen, auf dem Sie den Agenten installieren.

Erforderliche Komponenten

Der Agent benötigt die folgenden erforderlichen Komponenten.

- Stellen Sie bei VMware-Umgebungen sicher, dass Microsoft .NET Framework Version 2 oder höher auf dem Sicherungs-Proxysystem installiert ist und ausgeführt wird.
- Stellen Sie bei VMware-Umgebungen sicher, dass das VMware VCB-Framework auf dem Sicherungs-Proxysystem installiert ist.
- Für die Integration in VMware vSphere müssen die unten aufgelisteten Komponenten auf den Sicherungs-Proxy-Systemen installiert sein:
  - Diese Version von CA ARCserve Backup Agent für virtuelle Computer.
  - VMware Virtual Disk Development Kit (VDDK) 1.1 oder höher, VMware VCB Framework 1.5 Update 1 oder beides.

    Hinweis: Als Best Practice sollten Sie immer die aktuellste Version von VMware VCB und VMware VDDK installieren. Die aktuelle Version ist VMware VCB 1.5 Update 2 und VMware VDDK 1.2.1.

Unterstützte Konfigurationen für die Integration in VMware vSphere

Sie können den Agent in VMware vSphere auf den folgenden Betriebssystemen integrieren, wenn VMware VCB Framework auf dem Sicherungs-Proxy-System installiert ist:

- Windows Server 2003 x64
- Windows Server 2003 x86

- Windows Server 2008 x64
- Windows Server 2008 x86
- Windows Server 2008 R2

Sie können den Agent in VMware vSphere auf den folgenden Betriebssystemen integrieren, wenn VMware VDDK auf dem Sicherungs-Proxy-System installiert ist:

- Windows Server 2003 x64
- Windows Server 2003 x86
- Windows Server 2008 x64
- Windows Server 2008 x86
- Windows Server 2008 R2

Installieren und Konfigurieren des Agenten

Es gibt zwei Methoden, wie Sie den Agenten installieren können:

- Installieren Sie den Agenten bei der Installation von CA ARCserve Backup. Der Agent kann entsprechend den Standardvorgehensweisen für die Installation von Systemkomponenten, Agenten und Optionen von CA ARCserve Backup installiert werden.
- Installieren Sie den Agenten nach der Installation von CA ARCserve Backup. Mit der Agent-Bereitstellung können Sie den Agenten jederzeit nach der Installation von CA ARCserve Backup installieren.

  Hinweis: Weitere Informationen zum Installieren von Agenten mithilfe der Agent-Bereitstellung finden Sie im *Administrationshandbuch*.

Um den Agenten zu installieren und zu konfigurieren, müssen Sie zunächst folgende Aufgaben ausführen:

1. Befolgen Sie die Anweisungen zur Installation von CA ARCserve Backup im "*Implementierungshandbuch*".
2. Installieren Sie die für den Agenten erforderliche Anzahl von Lizenzen auf dem Primärserver oder dem eigenständigen Server.
3. Führen Sie die Konfigurationsaufgaben wie unter Aufgaben nach der Installation (siehe Seite 50) beschrieben aus.

Bereitstellen des Agenten für virtuelle Rechner unter Verwendung der Agent-Bereitstellung

Mit der CA ARCserve Backup Agent-Bereitstellung können Sie CA ARCserve Backup-Agenten auf lokalen VMs oder Remote-VMs installieren und aktualisieren. Bei der Methode zur Bereitstellung virtueller Rechner können Sie die Agenten angeben, die Sie auf lokalen VMs oder Remote-VMs installieren oder aktualisieren möchten. Durch diese Methode wird sichergestellt, dass alle in Ihrer CA ARCserve Backup-Umgebung auf VMs ausgeführten Agenten die gleiche Versionsnummer aufweisen wie der CA ARCserve Backup-Server.

Beachten Sie folgende Einschränkungen:

- Um einen Agenten auf einer VM zu installieren oder zu aktualisieren, muss die VM ausgeführt werden.
- Die Agent-Bereitstellung installiert und aktualisiert Agenten auf allen VMs, die sich innerhalb des ESX/ESXi-Serversystems und des Hyper-V-Hostsystems befinden.

So stellen Sie mittels der VM-Bereitstellung CA ARCserve Backup-Agenten auf VMs bereit:

1. Öffnen Sie die CA ARCserve Backup-Managerkonsole.

   Wählen Sie im Menü "Schnellstart" die Option "Verwaltung" aus, und klicken Sie auf "Agent-Bereitstellung".

   Die CA ARCserve Backup-Agent-Bereitstellung wird gestartet und das Dialogfeld "Anmeldeserver" geöffnet.

2. Füllen Sie die erforderlichen Felder in diesem Dialogfeld aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Methoden" wird geöffnet.

3. Wählen Sie im Dialogfeld "Methoden" die Option "Bereitstellung virtueller Rechner" aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Komponenten" wird geöffnet.

4. Wählen Sie im Dialogfeld "Komponenten" die Agenten aus, die Sie auf allen Remote-Hosts installieren möchten, und klicken Sie auf "Weiter".

   Das Dialogfeld "Hostinformationen" wird angezeigt.

5. Geben Sie auf eine der folgenden Arten die Namen der Remote-Hosts an, auf denen sich die VMs befinden:

   - Klicken Sie auf "Importieren", um eine Liste mit Remote-Hosts aus einer Textdatei zu importieren.

     Hinweis: Die Hostnamen müssen durch einen Zeilenumbruch voneinander abgetrennt werden. Sie können mehrere Textdateien importieren, die Gesamtanzahl der Remote-Hosts darf jedoch maximal 1000 betragen.

     Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

   - Klicken Sie auf "Aktualisieren", um die vorhandenen VMs aus der CA ARCserve Backup-Datenbank zu importieren.

     Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

   - Geben Sie den Namen des Remote-Hosts im Feld "Hostname" an, und klicken Sie auf "Hinzufügen".

     Hinweis: Wiederholen Sie diesen Schritt, bis alle erforderlichen Hostnamen in der Spalte "Host" angezeigt werden.

     Sobald die Hostnamen in der Spalte "Host" angezeigt werden, fahren Sie mit dem folgenden Schritt fort.

   Hinweis: Sie können bis zu 1000 Remote-Hosts angeben. Wenn Sie Agenten auf mehr als 1000 Remote-Hosts bereitstellen möchten, können Sie die Agent-Bereitstellung neu starten und diese Aufgabe wiederholen, oder Sie können die Agent-Bereitstellung von einem alternativen CA ARCserve Backup-Primärserver oder -Standalone-Server ausführen.

6. Geben Sie wie folgt den Benutzernamen und das Kennwort für die Remote-Hosts an:

   a. Klicken Sie in das Feld "Benutzername" (neben dem Hostnamen), und geben Sie den Benutzernamen in folgendem Format an:

      `<Domäne>\<Benutzername>`

   b. Klicken Sie in das Feld "Kennwort", und geben Sie das entsprechende Kennwort ein.

   c. Wiederholen Sie diesen Schritt, bis Sie den Benutzernamen und das Kennwort für alle Remote-Hosts angegeben haben.

   Falls Benutzername und Kennwort für alle Remote-Hosts identisch sind, geben Sie optional den Benutzernamen im Feld "Benutzer" ein (<Domäne>\<Benutzername>) und das Kennwort im Feld "Kennwort", stellen Sie sicher, dass alle Kontrollkästchen aktiviert sind, und klicken Sie dann auf "Anmeldeinformationen anwenden".

   Der Benutzername und das Kennwort werden für alle Remote-Hosts in der Liste übernommen.

   Hinweis: Um einen Host von der Liste "Hosts und Anmeldeinformationen" zu entfernen, aktivieren Sie das Kontrollkästchen neben dem Host, den Sie entfernen möchten, und klicken Sie auf "Entfernen".

   Klicken Sie auf "Weiter", um fortzufahren.

   Die Agent-Bereitstellung überprüft den für alle festgelegten Hosts angegebenen Hostnamen, den Benutzernamen und das Kennwort. Wenn die Agent-Bereitstellung keinen Authentifizierungsfehler ermittelt, wird das Statusfeld auf "Ausstehend" gesetzt. Wenn die Agent-Bereitstellung einen Authentifizierungsfehler ermittelt, wird das Statusfeld auf "Fehlgeschlagen" gesetzt. Sie können dann auf "Fehlgeschlagen" klicken, um die Gründe für den Fehler zu ermitteln. Sie müssen alle gemeldeten Fehler korrigieren, um fortzufahren.

   Klicken Sie auf "Weiter".

7. Wenn das Statusfeld aller Hosts "Ausstehend" oder "Bestätigt" anzeigt, klicken Sie auf "Weiter".

   Das Dialogfeld "Setup-Zusammenfassung" wird geöffnet.

8. Überprüfen Sie im Dialogfeld "Setup-Zusammenfassung" die angegebenen Komponenten und Hostnamen.

   Klicken Sie auf "Weiter".

   Das Dialogfeld "Installationsstatus" wird geöffnet.

9. Klicken Sie im Dialogfeld "Installationsstatus" auf "Installieren".

   Die Agent-Bereitstellung installiert oder aktualisiert die CA ARCserve Backup-Agenten auf den angegebenen Hosts.

   Nach Abschluss aller Installationen und Aktualisierungen wird das Dialogfeld "Installationsbericht" geöffnet.

10. Wählen Sie eine der folgenden Vorgehensweisen:

    - Wenn bei einigen Remote-Hosts ein Neustart erforderlich ist, klicken Sie auf "Weiter".

      Das Dialogfenster "Neu starten" wird geöffnet. In ihm sind die Remote-Hosts angegeben, die einen Neustart erfordern.

      Klicken Sie auf "Neu starten".

      Fahren Sie mit dem nächsten Schritt fort.

    - Wenn bei keinem der Remote-Hosts ein Neustart erforderlich ist, klicken Sie auf "Fertig stellen", um die Aufgabe abzuschließen.

11. Aktivieren Sie im Dialogfeld "Neu starten" das Kontrollkästchen neben dem Remote-Host, den Sie jetzt neu starten möchten.

    Optional können Sie das Kontrollkästchen "Alles markieren" aktivieren, um alle Remote-Hosts jetzt zu starten.

    Klicken Sie auf "Neu starten".

    Die Agent-Bereitstellung führt nun einen Neustart für alle Remote-Hosts aus.

    Hinweis: Wenn Sie eine Liste der Remote-Hosts erstellen möchten, für die ein Neustart erforderlich ist, klicken Sie auf "Bericht über Neustart exportieren".

12. Wenn das Statusfeld aller Remote-Hosts "Abgeschlossen" anzeigt, klicken Sie auf "Fertig stellen".

Die CA ARCserve Backup-Agenten sind nun auf den VMs bereitgestellt.

Aufgaben nach der Installation

In den folgenden Abschnitten werden die Aufgaben beschrieben, die Sie nach der Installation durchführen müssen, um verschiedene Versionen von VMware ESX/ESXi- und vCenter Server-Systemen zu schützen. Zum Schutz von Hyper-V-basierten Systemen ist nach der Installation des Agenten keine weitere Konfiguration erforderlich.

Dieser Abschnitt enthält folgende Themen:

VMware vSphere-Integration – Aufgaben nach der Installation

Führen Sie für die Integration in VMware vSphere nach Bedarf die folgenden Aufgaben für Ihre VM-Infrastruktur aus:

1. Füllen Sie die CA ARCserve Backup-Datenbank (siehe Seite 50).
2. Legen Sie eine Sicherungsmethode fest (siehe Seite 51).
3. Lassen Sie zu, dass auf dem Sicherungs-Proxy-System Bereitstellungspunkte (Snapshots) verbleiben (siehe Seite 55).
4. Ändern Sie den Standard-Kommunikations-Port für VDDK (siehe Seite 56).
5. Legen Sie eine Protokollierungsebene für VCBMounter fest (siehe Seite 57).

Pflegen der CA ARCserve Backup-Datenbank

Das ARCserve VMware-Konfigurationstool ist ein Hilfsprogramm zum Sammeln von Daten, das die CA ARCserve Backup-Datenbank mit Informationen zu den VMs in Ihrer Umgebung auffüllt.

Weitere Informationen finden Sie unter Einpflegen von Informationen in die Datenbank mithilfe des ARCserve VMware-Konfigurationstools (siehe Seite 73).

Festlegen von Sicherungsmethoden

Im Agent können Sie eine der folgenden Methoden festlegen, um VM-Sicherungsdaten zu schützen:

- **VMware vSphere Web Services SDK und VMware VDDK**: Ermöglichen den Schutz der nachfolgenden Implementierungen:
  - ESX SERVER 3.5 und höher, wenn über vCenter Server 4.0 und höher verwaltet
  - VMware Virtual Center 2.5 und höher bis zu vCenter Server 4.0 verwalten ESX Server 3.5 und höher bis zu ESX Server 4.0

  Wichtig! Nachdem Sie den Agent standardmäßig installiert haben, bearbeitet CA ARCserve Backup Sicherungen mithilfe von VDDK, sofern VDDK im Sicherungs-Proxy-System installiert ist. Sie können jedoch angeben, dass für Sicherungen der VCB-Ansatz verwendet werden soll, und zwar durch Änderung der in diesem Thema erläuterten Registrierungsschlüssel.

- **VCB Framework**: Hiermit können VMs auf allen ESX Server-Systemen geschützt werden, die von der VCB Framework-Version unterstützt werden, die auf dem Sicherungs-Proxy-System installiert ist.

  Hinweis: VMware ESX Server 4.0 und VMware vCenter Server 4.0 werden nur durch VCB Framework 1.5 Update 1 (und Nachfolgerversionen) unterstützt.

Methode mit VMware-vSphere Webservices SDK und VMware VDDK

Beachten Sie das Folgendes, wenn Sie die Methode mit VMware vSphere Webservices SDK und VMware VDDK verwenden:

- VMware VDDK muss auf dem Sicherungs-Proxysystem installiert sein.
- Mit dieser Vorgehensweise nutzt CA ARCserve Backup VDDK zur Verarbeitung von Raw-Sicherungen (vollständige VM-Sicherungen) und Raw-Sicherungen (vollständige VM-Sicherungen) mit aktivierter Option "Wiederherstellung im Dateimodus zulassen", wenn VDDK und VCB auf dem Sicherungs-Proxy-System installiert sind. CA ARCserve Backup nutzt jedoch immer VCB Framework zur Durchführung von Sicherungen im Dateimodus, wenn VCB Framework und VDDK oder nur VCB Framework auf dem Sicherungs-Proxy-System installiert ist.

- CA ARCserve Backup sichert nur aktive Blöcke der Phase der vollständigen Sicherung bei Raw-Sicherungen (vollständiger virtueller Rechner) ohne oder mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" sowie gemischter Sicherungen mit aktivierter Option "Wiederherstellung im Dateimodus erlauben".

  Wenn die virtuellen Datenträger als Thick-Datenträger oder Thin-Datenträger bereitgestellt werden, erstellt CA ARCserve Backup Sicherungssitzungen, deren Größe ungefähr dem verwendeten Speicherplatz auf dem VM entspricht.

  CA ARCserve Backup unterstützt die Vorgehensweise der aktiven Blockanalyse nicht auf virtuellen Rechnern, die virtuelle Datenträger zur Partitionsgerätzuordnung (RDM) enthalten. Wenn CA ARCserve Backup virtuelle RDM-Datenträger erkennt, können Sie allerdings vollständige Sicherungen der virtuellen RDM-Datenträger übergeben und die Datenträger als normale Thick-Datenträger wiederherstellen.

  Hinweis: Wird eine der folgenden Warnmeldungen im Aktivitätsprotokoll angezeigt, wenn ein aktiver Blocksicherungsjob ausgeführt wird, können Sie die Meldungen ignorieren, da der Job trotzdem erfolgreich abschließen sollte.

  - AW0720: Bitmap für Datenträger konnte nicht erstellt werden. [Volle Datenträger inklusive nicht verwendeter Blöcke werden gesichert.]
  - AW0589: Verfolgung der Blockänderung für den virtuellen Rechner konnte nicht aktiviert werden. [Volle Datenträger inklusive nicht verwendeter Blöcke werden gesichert.]

  Beachten Sie Folgendes:

  - Aufgrund einer VMware-Beschränkung unterstützt der Agent die Sicherung von Partitionsgerätzuordnung (RDM) in physisch kompatiblem Modus nicht.
  - Überprüfen Sie bei der ersten Sicherung von virtuellen Rechnern mithilfe dieser Vorgehensweise (aktive Blocksicherung), dass keine Snapshots auf den virtuellen Rechnern vorhanden sind. Für alle nachfolgenden Sicherungen kann es einen oder mehrere Snapshots auf den virtuellen Rechnern geben.
  - CA ARCserve Backup führt aktive Blocksicherungen auf virtuellen Rechnern durch, die auf VMware-Hardware der Version 7 und den folgenden VMware-Plattformen ausgeführt werden:
    - ESX Server 4.0 oder höher
    - vCenter Server 4.0 oder höher

- Bei Sicherungsvorgängen wird der Snapshot im Bereitstellungsverzeichnis gespeichert, das mit dem ARCserve VMware-Konfigurationstool angegeben wurde.
- CA ARCserve Backup nutzt VDDK zur Datenwiederherstellung, wenn die VM-Daten unter Verwendung von VDDK gesichert werden.

  Hinweis: Es ist nicht erforderlich, dass VMware Converter Daten virtueller Rechner wiederherstellt, die mithilfe von VDDK gesichert wurden.
- Bei der Sicherung wird eine Datei namens "vmconfig.dat" im Binärformat erstellt, die die VM-Konfigurationsdetails enthält.

  Hinweis: Versuchen Sie keinesfalls, vmconfig.dat zu ändern.
- Bei der Sicherung werden keine Katalogdateien erstellt oder aktualisiert.
- Im Bereitstellungspunktverzeichnis werden keine Dateien für das bereitgestellte Volume angezeigt. Dieses Verhalten tritt auf, weil VDDK keine Volumes in einem Verzeichnis bereitstellt bzw. Volumes keinem Laufwerksbuchstaben zuordnet.
- Bei der Sicherung werden Datenträgerdateien mit der Dateigröße Null im Bereitstellungsverzeichnis für Raw-Sicherungen (vollständige VM-Sicherungen) sowie Raw-Sicherungen mit aktivierter Option "Wiederherstellung auf Dateiebene erlauben" erstellt.

  Hinweis: Versuchen Sie nicht, die Datenträgerdateien zu ändern.

Beachten Sie bei Sicherungen auf Dateiebene mit der **VCB-Framework**-Methode *oder* der Methode mit **VMware vSphere Webservices SDK und VMware VDDK** das folgende Verhalten:

- Bei der Sicherung werden keine Katalogdateien erstellt oder aktualisiert.
- Bei der Sicherung wird im Bereitstellungspunktverzeichnis ein untergeordneter Datenträger erstellt.

Wichtig! Wenn VM-Daten mit dem VDDK-Ansatz geschützt werden sollen, muss VMware VDDK auf dem Sicherungs-Proxy-System installiert sein. Ebenso gilt: Wenn VM-Daten mit dem VCB-Ansatz geschützt werden sollen, muss VMware VCB-Framework auf dem Sicherungs-Proxy-System installiert sein.

So legen Sie eine Sicherungsmethode fest

1. Öffnen Sie den Windows-Registrierungs-Editor.

   Ändern Sie nach Bedarf die folgenden Registrierungsschlüssel, indem Sie die angegebenen Werte verwenden.

   - **Schlüsselname--**useVCBFor35

     Hiermit können Sie angeben, welche VMware-Anwendung für Sicherungsvorgänge auf ESX Server 3.5-Systemen verwendet werden soll, wenn VCB-Framework und VDDK auf dem Sicherungs-Proxy-System installiert sind.

     Pfad

     `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters`

     Typ

     REG_DWORD

     Standardwert

     0 (Daten unter Verwendung von VDDK sichern)

     Hinweis: Wenn VMs mit VCB-Framework geschützt werden sollen, wenn ESX Server 3.5 auf dem Sicherungs-Proxy-System installiert ist, legen Sie diesen Wert auf 1 fest.

   - **Schlüsselname--**useVCBFor40

     Hiermit können Sie angeben, welche VMware-Anwendung für Sicherungsvorgänge auf ESX Server 4.0-Systemen verwendet werden soll, wenn VCB-Framework und VDDK auf dem Sicherungs-Proxy-System installiert sind.

     Pfad

     `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters`

     Typ

     REG_DWORD

     Standardwert

     0 (Daten unter Verwendung von VDDK sichern)

     Hinweis: Wenn VMs mit VCB-Framework geschützt werden sollen, wenn ESX Server 4.0 auf dem Sicherungs-Proxy-System installiert ist, legen Sie diesen Wert auf 1 fest.

2. Schließen Sie den Windows-Registrierungs-Editor.

Zulassen, dass auf dem Sicherungs-Proxy-System Bereitstellungspunkte (Snapshots) verbleiben

Standardmäßig löscht CA ARCserve Backup das Bereitstellungspunktverzeichnis (Snapshot) auf dem Sicherungs-Proxy-System, nachdem die Sicherung der VMs erfolgreich abgeschlossen wurde. Wenn die Sicherung fehlschlägt und der Snapshot nicht vom Sicherungs-Proxy-System gelöscht wird, löscht CA ARCserve Backup das Bereitstellungsverzeichnis bei der nächsten Durchführung einer Sicherung. Mit diesem Ansatz wird sichergestellt, dass der Agent den für die Durchführung von VM-Sicherungen erforderlichen Speicherplatz minimiert.

Sie haben auch die Möglichkeit, den Snapshot auf dem Sicherungs-Proxy-System zu belassen, wenn alle der nachfolgend aufgeführten Bedingungen in Ihrer VM-Sicherungsumgebung erfüllt sind:

- Sie führen die Sicherung von Daten mithilfe der Funktion für die Deduplizierung durch.
- Die Deduplizierungsgeräte fungieren als Datenspeicher, die sich auf dem Sicherungs-Proxy-System befinden.
- Das Freigeben von Speicherplatz auf dem Sicherungs-Proxy-System ist keine Voraussetzung.

Mit diesem Ansatz können Sie den Zeitaufwand für die Wiederherstellung von VM-Daten verringern.

Wenn auf dem Sicherungs-Proxysystem Bereitstellungspunkte verbleiben, folgte deren Benennung durch CA ARCserve Backup den folgenden Konventionen:

- Erfolgreiche Sicherungen--CA ARCserve Backup benennt das Bereitstellungspunktverzeichnis wie folgt um:

  ```
  <VM-Name>_J<JobID>_S<SessionID>_datum_uhrzeit
  ```

  Hinweis: CA ARCserve Backup benennt das Bereitstellungspunktverzeichnis um, wenn die Sicherung abgeschlossen ist.

- Erfolglose und unvollständige Sicherungen: Beim nächsten Sicherungsjob, der für den virtuellen Rechner mit demselben Sicherungs-Proxy-System ausgeführt wird, benennt CA ARCserve Backup das Bereitstellungspunktverzeichnis auf folgende Art um:

  ```
  <VM-Name>_J<JobID>_S<SessionID>_err_datum_uhrzeit
  ```

Zulassen, dass auf dem Sicherungs-Proxy-System Bereitstellungspunkte (Snapshots) verbleiben

1. Klicken Sie im Windows-Startmenü auf die Option "Ausführen".

   Das Dialogfeld "Ausführen" wird geöffnet.

2. Geben Sie im Feld "Öffnen" "regedit" ein.

   Der Registrierungs-Editor von Windows wird geöffnet.

3. Wechseln Sie zu folgendem Schlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve
   Backup\ClientAgent\Parameters
   ```

   Die Werte des Schlüssels werden angezeigt.

4. Wählen Sie im Bearbeitungsmenü die Option "Neu" aus, und klicken Sie auf "DWORD-Wert".

   Vergeben Sie für den DWORD-Wert den Namen retainVCBMountDir.

   Klicken Sie mit der rechten Maustaste auf retainVCBMountDir, und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

5. Geben Sie im Datenfeld für den Wert "1" ein, und klicken Sie dann auf "OK".

   Der Schlüssel wird erstellt.

6. Schließen Sie den Registrierungs-Editor.

Ändern Sie den Standard-Kommunikations-Port für VDDK.

Standardmäßig wird die Kommunikation von VDDK über Port 902 abgewickelt. Sie können den Port ändern, wenn die VDDK-Kommunikation über einen gesicherten Port oder einen bestimmten, für Ihr Unternehmen erforderlichen Port ablaufen muss.

In den folgenden Schritten wird beschrieben, wie der standardmäßige VDDK-Kommunikations-Port geändert wird.

So ändern Sie den standardmäßigen VDDK-Kommunikations-Port:

1. Klicken Sie im Windows-Startmenü auf die Option "Ausführen".

   Das Dialogfeld "Ausführen" wird geöffnet.

2. Geben Sie im Feld "Öffnen" "regedit" ein.

   Der Registrierungs-Editor von Windows wird geöffnet.

3. Wechseln Sie zu folgendem Schlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters`

   Die Werte des Schlüssels werden angezeigt.

4. Klicken Sie mit der rechten Maustaste auf "VDDKPort", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

   Hinweis: Der Standardwert von "VDDKPort" lautet "902".

   Geben Sie im Feld "Wert" einen Kommunikations-Port an, und klicken Sie auf "OK".

   Der Schlüssel wird geändert.

5. Schließen Sie den Registrierungs-Editor.

Angeben einer Protokollebene für VCBMounter

Mit der Protokolldatei vcbmounteroutput_xxx.log können Sie die Details zu Ladevorgängen anzeigen, die sich auf VM-Sicherungen beziehen. Optional können Sie in CA ARCserve Backup den Umfang der Details angeben, die in der Protokolldatei beschrieben werden sollen.

So geben Sie eine Protokollebene für VCBMounter an:

1. Klicken Sie im Windows-Startmenü auf die Option "Ausführen".

   Das Dialogfeld "Ausführen" wird geöffnet.

2. Geben Sie im Feld "Öffnen" "regedit" ein.

   Der Registrierungs-Editor von Windows wird geöffnet.

3. Wechseln Sie zu folgendem Schlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters`

   Die Werte des Schlüssels werden angezeigt.

4. Wählen Sie im Bearbeitungsmenü die Option "Neu" aus, und klicken Sie auf "DWORD-Wert".

   Benennen Sie den DWORD-Wert mit "VcbMountLogLevel".

   Klicken Sie mit der rechten Maustaste auf "VcbMountLogLevel", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

5. Geben Sie im Feld "Wert" eine Protokollebene von 1 bis 6 an.

   Hinweis: Je höher die Protokollebene, desto detailliertere Informationen werden im Protokoll angegeben.

   Klicken Sie auf "OK".

   Der Schlüssel wird erstellt und die Protokollebene angewendet.

6. Schließen Sie den Registrierungs-Editor.

Konfigurieren der Anzahl der gleichzeitigen Lesevorgänge mithilfe von VDDK

Mit CA ARCserve Backup können Sie die Anzahl der gleichzeitigen Lesevorgänge auf virtuellen VM-Datenträgern vergrößern und verringern, wenn Sie Sicherungen mit VDDK durchführen. Die Möglichkeit, die Anzahl der gleichzeitigen Lesevorgänge zu vergrößern und zu verringern, ist nützlich, um das allgemeine Sicherungszeitfenster zu minimieren. Sie vergrößern und verringern die Anzahl der gleichzeitigen Lesevorgänge in Abhängigkeit von der Anzahl der VMs, die Sie als Teil des gleichen Jobs oder mehrerer Jobs sichern, die von einem Sicherungs-Proxy-System ausgeführt werden. Um die Anzahl der gleichzeitigen Lesevorgänge anzugeben, erstellen oder ändern Sie den folgenden Schlüssel (falls bereits in der Registrierung vorhanden):

Pfad

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe
Backup\ClientAgent\Parameters
```

Schlüsselname

```
VmdkReaderCount
```

Standardwert

```
4 (Daten unter Verwendung von VDDK sichern)
```

Max.-Wert

```
8
```

Hinzufügen oder Entfernen bestimmter VM-Daten zu/aus der CA ARCserve Backup-Datenbank

CA ARCserve Backup bietet Befehlszeilenargumente, mit denen Sie bestimmte VM-Daten zur CA ARCserve Backup-Datenbank hinzufügen oder daraus entfernen können. Sie können die Argumente verwenden, wenn Sie den Namen des bestimmten virtuellen Rechners kennen, den Sie zur CA ARCserve Backup-Datenbank hinzufügen oder daraus entfernen möchten. Dies sind die Befehlszeilenargumente:

```
-insertvm <VM-Name>
-deletevm <VM-Name>
```

Hinweis: Sie können "-insertVM" und "-deleteVM" mit dem VMware-Befehlszeilenhilfsprogramm (ca_vcbpopulateDB) und dem Hyper-V-Befehlszeilenhilfsprogramm (ca_msvmpopulateDB) verwenden. Weitere Informationen zu Hilfsprogrammen finden Sie im *Befehlszeilen-Referenzhandbuch*.

So fügen Sie VM-Daten zur CA ARCserve Backup-Datenbank hinzu oder entfernen Sie daraus:

1. Rufen Sie die Windows-Eingabeaufforderung auf.

   Ändern Sie das Verzeichnis auf das Verzeichnis, unter dem der Client Agent für Windows installiert ist.

2. Führen Sie unter Verwendung der folgenden Syntax "ca_vcbpopulateDB" (VMware-VMs) oder "ca_msvmpopulateDB" (Hyper-V-VMs) aus:

   -insertvm <VM-Name>

   Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine VMware-VM mit Hostnamen VM-001 in die CA ARCserve Backup-Datenbank einzufügen:

   ```
   ca_vcbpopulatedb.exe -Primary ARCServe1 -carootUser caroot -carootPass ca
   -esxServer ESXServer1 -esxUser root -esxUserPass rootpass -insertVM VM-
   001 -debug
   ```

   Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine Hyper-V-VM mit Hostnamen VM-001 in die CA ARCserve Backup-Datenbank einzufügen:

   ```
   ca_msvmpopulatedb.exe –Primary ARCServe1 –insertVM VM-001 –debug 1
   ```

   -deletevm <VM-Name>

   Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine VMware-VM mit Hostnamen VM-001 aus der CA ARCserve Backup-Datenbank zu löschen:

   ```
   ca_vcbpopulatedb.exe -Primary ARCServe1 -carootUser caroot -carootPass ca
   -esxServer ESXServer1 -esxUser root -esxUserPass rootpass -deleteVM VM-
   001 -debug
   ```

   Im folgenden Beispiel wird die Syntax beschrieben, die erforderlich ist, um eine Hyper-V-VM mit Hostnamen VM-001 aus der CA ARCserve Backup-Datenbank zu löschen:

   ```
   ca_msvmpopulatedb.exe –Primary ARCServe1 –deleteVM VM-001 –debug 1
   ```

So verwenden Sie den Transportmodus "hotadd" von VMware:

Der Transportmodus "hotadd" von VMware ist eine Option in VMware Consolidated Backup r1.5, die verwendet werden kann, wenn VCB auf einer VM installiert ist.

Hinweis: Weitere Informationen zur Verwendung des Transportmodus "hotadd" finden Sie im Handbuch *Virtual Machine Backup Guide* unter www.vmware.com.

Beachten Sie folgende Punkte, wenn Sie den Transportmodus "hotadd" von VMware in Ihrer Umgebung verwenden.

- Der Agent unterstützt den VMware-Hotadd-Transportmodus unter Verwendung von VCB auf virtuellen Rechnern, auf denen Folgendes ausgeführt wird:
  - ESX Server 3.5 oder höher
  - vCenter Server 2.5 oder höher
- Das Sicherungs-Proxysystem muss auf einer VM konfiguriert sein.
- Die VCB-Helper-VM muss ohne die Verwendung virtueller Festplatten erstellt werden.
- Falls Sie nur auf lokalen Speichergeräten sichern, muss auf allen VMware ESX Server-Hostsystemen ein VCB-Proxy-VM konfiguriert sein.
- Sie müssen DWORD UseHotadd in dem Registrierungsschlüssel erstellen, der auf das Sicherungs-Proxysystem folgt.

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve
  Backup\ClientAgent\Parameters
  ```

  DWORD: UseHotadd

  Wert: 1

Beenden von Vorgängen bei abgelaufenen SSL-Zertifikaten

Sicherungs-Proxy-Systeme können so konfiguriert werden, dass bei der Kommunikation mit VMware ESX-Hostsystemen gültige SSL-Zertifikate bezogen werden. Standardmäßig setzt der Agent VM-basierte Vorgänge (wie etwa die automatische Aufnahme, Sicherungen und Wiederherstellungen) auch bei ungültigen oder abgelaufenen SSL-Zertifikaten fort. Hiermit soll ein kontinuierlicher Schutz der virtuellen Rechner in Ihrer Umgebung gewährleistet werden.

Falls dieses Verhalten nicht den Erfordernissen Ihrer Organisation entspricht, können Sie selbst festlegen, was geschehen soll, wenn der Agent auf dem VMware ESX-Hostsystem ungültige oder abgelaufene SSL-Zertifikate ermittelt.

So beenden Sie Vorgänge bei abgelaufenen SSL-Zertifikaten:

1. Öffnen Sie den Registrierungs-Editor, und rufen Sie den folgenden Registrierungsschlüssel auf:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA Arcserve
   Backup\ClientAgent\Parameters
   ```

2. Erstellen Sie den Registrierungsschlüsselwert "SSLCertificateVerify" mit dem Typ DWORD.

   Legen Sie als Wert für den Schlüssel "SSLCertificateVerify" "1" fest.

3. Schließen Sie den Registrierungs-Editor.

Festlegen benutzerdefinierter HTTP/HTTPS-Kommunikationsports

VMware vCenter Server Virtual Infrastructure (VI) SDK verwendet HTTP-Port 80 und HTTPS-Port 443 für die Kommunikation mit Web Services. Diese Ports können mit den von den Microsoft-Internetinformationsdiensten (IIS) verwendeten Kommunikationsports im Konflikt stehen. Um Portkonflikte zu vermeiden, ermöglichen VMware vCenter Server und Mware ESX Server die Angabe benutzerdefinierter VI SDK Web Services-Ports. Falls Sie jedoch die VI SDK Web Services-Ports ändern, kann CA ARCserve Backup die VM-Daten möglicherweise nicht auf das Sicherungs-Proxy-System laden, und Sicherungen können fehlschlagen.

Um dieses Problem zu beheben, ermöglicht CA ARCserve Backup das Erstellen eines Satzes von benutzerdefinierten HTTP- und HTTPS-Kommunikationsports, die zulassen, dass CA ARCserve Backup die VM-Daten auf das Sicherungs-Proxy-System lädt.

Hinweis: Informationen über das Konfigurieren von VI SDK Web Services-Ports auf VMware vCenter Server- und VMware ESX Server-Systemen finden Sie in der VMware-Dokumentation.

Die folgende Abhilfe stellt eine globale Änderung dar, die sich auf ESX- und vCenter-Serversysteme auswirkt, die Sie unter Verwendung eines bestimmten Sicherungs-Proxy-Systems sichern. Die Best Practice ist daher, ein dediziertes Sicherungs-Proxy-System zu identifizieren, das verwendet wird, um Daten auf VMware vCenter-Serversysteme zu laden, die einen benutzerdefinierten VI SDK-Port enthalten.

So legen Sie benutzerdefinierte HTTP/HTTPs-Kommunikationsports fest

1. Melden Sie sich beim Sicherungs-Proxy-System an.
2. Öffnen Sie den Editor der Windows Registry.

3. Erstellen Sie folgenden Registrierungsschlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\ClientAgent\Parameters\VIHTTPPort`

   Klicken Sie mit der rechten Maustaste auf "VIHTTPPort", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

4. Geben Sie im Datenfeld "Wert" die benutzerdefinierte HTTP-Kommunikationsportnummer an, die mit VMware vCenter Server konfiguriert wurde.

   Klicken Sie auf "OK".

   Die Portnummer wird angewandt.

5. Erstellen Sie folgenden Registrierungsschlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\ClientAgent\Parameters\VIHTTPSPort`

   Klicken Sie mit der rechten Maustaste auf "VIHTTPSPort", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

6. Geben Sie im Datenfeld "Wert" die benutzerdefinierte HTTPS-Kommunikationsportnummer an, die mit VMware vCenter Server konfiguriert wurde.

   Klicken Sie auf "OK".

   Die Portnummer wird angewandt.

Konfigurieren des Agenten, um MAC-Adressen nach der Wiederherstellung von virtuellen Rechnern beizubehalten

Der Prozess zur Wiederherstellung virtueller Rechner unter Verwendung der VM-Wiederherstellungsmethode ermöglicht es Ihnen möglicherweise nicht, die MAC-Adressen der virtuellen Rechner (wenn eine MAC-Adresse definiert wurde) beizubehalten, nachdem die Wiederherstellung abgeschlossen wurde. CA ARCserve Backup reagiert in dieser Form in Sicherungsumgebungen, die diese Vorgehensweise zur Sicherung von VMware VDDK verwenden.

Hinweis: Die vSphere-Client-Anwendung ermöglicht es Ihnen, zu überprüfen, ob die MAC-Adresse nach der Wiederherstellung virtueller Rechner beibehalten wurden.

Führen Sie die folgenden Schritte nur aus, wenn Sie die Vorgehensweise zur Sicherung von VMware VDDK (siehe Seite 51) in Ihrer Sicherungsumgebung verwenden.

So konfigurieren Sie den Agenten, um MAC-Adressen nach der Wiederherstellung von virtuellen Rechnern beizubehalten

1. Melden Sie sich bei dem Computer an, auf dem der Agent installiert ist, und öffnen Sie den Windows-Registrierungs-Editor.
2. Suchen Sie folgenden Eintrag:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Client Agent\Parameters
   ```

3. Erstellen Sie den folgenden Schlüssel:

   Schlüsselname:

   `RetainMACForVDDK`

   Geben Sie einen der folgenden Werte für den Schlüssel an:

   - **1** - MAC-Adresse beibehalten
   - **0** - MAC-Adresse nicht beibehalten

4. Speichern Sie den Schlüssel und schließen Sie den Windows-Registrierungs-Editor.

Konfigurieren des Agenten, um die Ressourcenzuordnung des Datenträgers nach Wiederherstellung von virtuellen Rechnern beizubehalten

Der Prozess zur Wiederherstellung virtueller Rechner unter Verwendung der VM-Wiederherstellungsmethode ermöglicht es Ihnen möglicherweise nicht, die Ressourcenzuordnung des Datenträgers für virtuelle Rechner beizubehalten. Sie können die Ressourcenzuordnung des Datenträgers nach der Wiederherstellung virtueller Rechner nur beibehalten, wenn Sie die Vorgehensweise zur Sicherung von VMware VDDK (siehe Seite 51) in Ihrer Sicherungsumgebung verwenden.

So konfigurieren Sie Agenten, um die Ressourcenzuordnung des Datenträgers nach Wiederherstellung von virtuellen Rechnern beizubehalten

1. Melden Sie sich bei dem Computer an, auf dem der Agent installiert ist, und öffnen Sie den Windows-Registrierungs-Editor.
2. Suchen Sie den folgenden Registrierungsschlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Client Agent\Parameters
   ```
3. Erstellen Sie den folgenden Schlüssel:

   Schlüsselname:

   ```
   RetainDiskResourceForVDDK
   ```

   Geben Sie einen der folgenden DWORD-Werte für den Schlüssel an:

   - **1** - Ressourcenzuordnung des Datenträgers beibehalten
   - **0** - Ressourcenzuordnung des Datenträgers nicht beibehalten
4. Speichern Sie den Schlüssel und schließen Sie den Windows-Registrierungs-Editor.

Aktivieren des Debugging für VDDK-Jobs

Mit CA ARCserve Backup können Sie Debug-Protokolle für VDDK-Sicherungen aktivieren. Debug-Protokolle können verwendet werden, um Fehler bei Sicherungs- und Wiederherstellungsvorgängen zu beheben.

So aktivieren Sie das Debugging für VDDK-Jobs

1. Melden Sie sich beim Sicherungs-Proxy-System an.

   Öffnen Sie den Editor der Windows Registry.

   Suchen Sie folgenden Registrierungsschlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe
   Backup\ClientAgent\Parameters\Debug
   ```

   Klicken Sie mit der rechten Maustaste auf "Debug", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.

2. Geben Sie im Feld "Wert" 1 an.

   CA ARCserve Backup generiert eine Protokolldatei auf dem Sicherungs-Proxy-System im Verzeichnis "ARCserve Backup Client Agent für Windows\Protokoll" namens "VMDKIOXXXX.log".

Deinstallieren des Agenten

Als Best Practice können Sie in der Windows-Systemsteuerung "Software" verwenden, um den Agent zu deinstallieren. Mit der CA ARCserve Backup-Deinstallationsroutine können Sie den Agent und eine beliebige Kombination von CA ARCserve Backup-Komponenten deinstallieren.

So deinstallieren Sie den Agenten:

1. Öffnen Sie die Windows-Systemsteuerung, und doppelklicken Sie auf die Option "Software".

   Suchen und wählen Sie CA ARCserve Backup.

   Klicken Sie auf "Deinstallieren".

   Das CA ARCserve Backup-Dialogfeld für das Entfernen von Anwendungen und Komponenten wird geöffnet.

2. Wählen Sie "CA ARCserve Backup Agent für virtuelle Rechner" aus.

   Klicken Sie auf "Weiter".

   Das CA ARCserve Backup-Dialogfeld für das Entfernen von Anwendungen und Meldungen wird geöffnet.

3. Klicken Sie auf "Weiter".

   Das CA ARCserve Backup-Dialogfeld für das Entfernen von Anwendungen wird geöffnet.

4. Setzen Sie ein Häkchen neben "Aktivieren Sie dieses Kontrollkästchen", um zu bestätigen, dass Sie die angegebenen Komponenten von Ihrem Computer entfernen wollen, und klicken Sie auf "Entfernen".

   Der Agent wird deinstalliert.

Kapitel 3: Auffüllen der CA ARCserve Backup-Datenbank

Dieses Kapitel enthält folgende Themen:

Geben Sie den Namen des CA ARCserve Backup-Servers an.

Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben.

Diese Aufgabe entfällt, wenn Sie den CA ARCserve Backup Agenten für virtuelle Rechner mithilfe des Agent-Bereitstellungstools auf Ihren virtuellen Rechnern installiert haben. Weitere Informationen finden Sie unter Bereitstellen von Agenten für virtuelle Rechner unter Verwendung der VM-Bereitstellung (siehe Seite 46).

Hinweis: Die folgenden Schritte gelten für VMware- und Hyper-V-VMs.

So geben Sie den Namen des CA ARCserve Backup-Servers an:

1. Melden Sie sich bei der VM an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.

   Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".

   Das Dialogfeld "Backup Agent – Verwaltung" wird geöffnet.

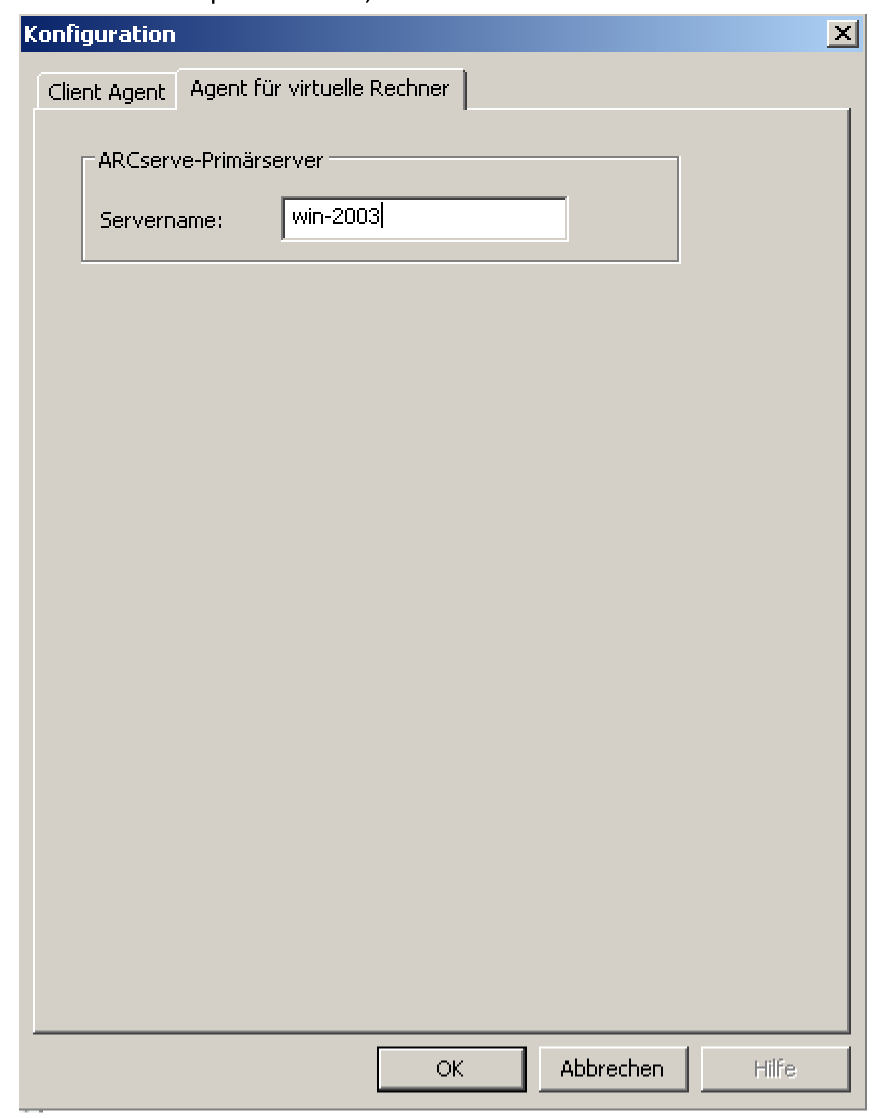
2. Wählen Sie in der Drop-down-Liste die Option "CA ARCserve Backup Client Agent", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

   Das Dialogfeld "Konfiguration" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Agent für virtuelle Rechner".

   Geben Sie im Feld "Servername" den Hostnamen oder die IP-Adresse des CA ARCserve Backup-Servers ein, der diese VM schützt.



   Klicken Sie auf "OK".

Der Name des CA ARCserve Backup-Servers wird gespeichert.

Hinweis: Wiederholen Sie diese Schritte nach Bedarf auf allen VMs in Ihrer CA ARCserve Backup-Umgebung.

Festlegen eines temporären VM-Ladeorts

Um Informationen zu den virtuellen Rechnern in Ihrer VMware-Sicherungsumgebung in die CA ARCserve Backup-Datenbank aufzunehmen, benötigt CA ARCserve Backup einen Speicherort, um die Sicherungsinformationen temporär zu speichern, während das ARCserve VMware-Konfigurationstool ausgeführt wird.

Standardmäßig speichert CA ARCserve Backup die temporären Sicherungsinformationen an dem Speicherort, der auf das Sicherungs-Proxy-System folgt:

```
C:\Programme\CA\ARCserve Backup Client Agent for Windows
```

Hinweis: Zur Durchführung von Raw-Sicherungen (vollständige VM-Sicherungen) und Raw-Sicherungen, bei denen die Option "Wiederherstellung auf Dateiebene erlauben" aktiviert ist, müssen Sie mindestens den auf dem Laufwerk verwendeten Festplattenspeicher oder Speicherplatz bis zur maximalen Laufwerkgröße des Laufwerks reservieren, um die im vorübergehenden VM-Ladeort gespeicherten Daten aufzunehmen. Bei Sicherungen auf Dateiebene ist die Größe des verfügbaren Festplattenspeichers unabhängig von der Größe des virtuellen Rechners. Sicherungen im Dateimodus benötigen einen minimalen verfügbaren Festplattenspeicher am temporären Ladespeicherort.

Führen Sie folgende Schritte aus, um einen anderen Speicherort für den temporären VM-Ladeort auf dem Sicherungs-Proxy-System festzulegen.

Beachten Sie Folgendes:

- Der temporäre VM-Ladeort muss sich auf dem Sicherungs-Proxy-System befinden.
- Die Verwendung zugeordneter Laufwerke auf dem Sicherungs-Proxy-System für den temporären VM-Ladeort wird von CA ARCserve Backup nicht unterstützt.

So legen Sie einen temporären VM-Ladeort fest:

1. Melden Sie sich beim Sicherungs-Proxysystem an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.

   Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".

   Das Dialogfeld "Backup Agent-Verwaltung" wird geöffnet.

2. Wählen Sie in der Drop-down-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

   Das ARCserve-Konfigurationstool für VMware wird geöffnet.

3. Geben Sie im Feld "Temporärer VM-Ladeort" den Pfad zu dem Standort an, an dem Sie die Daten laden möchten.

4. Klicken Sie auf "Festlegen".

   Der temporäre VM-Ladeort ist eingestellt.

5. Klicken Sie auf "Schließen".

   Das ARCserve VMware-Konfigurationstool wird beendet.

Einpflegen von Informationen in die Datenbank mithilfe des ARCserve-Konfigurationstools für VMware

Das ARCserve VMware-Konfigurationstool ist ein Hilfsprogramm zum Sammeln von Daten, das die CA ARCserve Backup-Datenbank mit Informationen zu den VMs auf Ihren VMware ESX-Hostsystemen auffüllt. In dieses Tool ist ein Befehlszeilendienstprogramm namens "ca_vcbpopulatedb" integriert, das im Hintergrund ausgeführt wird und Informationen zu den VMs in die ARCserve-Datenbank einpflegt. Das Konfigurationstool sammelt folgende Informationen:

- VCB-Sicherungs-Proxynamen
- VMware ESX-Hostnamen oder VMware vCenter-Servernamen
- VM-Hostnamen
- Namen der Volumes auf den VMs in Windows-Systemen

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren VM-Systemen füllen. Hierfür müssen Sie das ARCserve-Konfigurationstool für VMware auf dem Sicherungs-Proxysystem ausführen.

Nachdem Sie das ARCserve VMware-Konfigurationstool ausgeführt und einen Sicherungsjob für die Daten auf den virtuellen Rechnern übergeben haben, wird die CA ARCserve Backup-Datenbank automatisch mit den Informationen über die virtuellen Rechner gefüllt, die bei der Ausführung des Konfigurationstools angegeben wurden. Mit der Option für das automatische Auffüllen können Sie sicherstellen, dass der Sicherungs-Manager richtig durchsucht wird und die aktuellen Daten auf den virtuellen Rechnern gesichert werden. CA ARCserve Backup füllt die Datenbank standardmäßig automatisch in 24-Stunden-Abständen nach Abschluss der Sicherung mit aktualisierten Daten.

So pflegen Sie Informationen in die Datenbank mithilfe des ARCserve-Konfigurationstools für VMware ein

1. Stellen Sie sicher, dass die VMs in den VMware ESX-Hostsystemen ausgeführt werden.

   Hinweis: Wenn die VMs nicht ausgeführt werden, lädt das ARCserve-Konfigurationstool für VMware keine Daten in die CA ARCserve Backup-Datenbank, und Sie können die VMs in den VMware ESX-Hostsystemen nicht richtig durchsuchen und sichern.

2. Melden Sie sich beim Sicherungs-Proxysystem an, und öffnen Sie den Bereich für die Backup Agent-Verwaltung.

   Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".

   Das Dialogfeld "Backup Agent – Verwaltung" wird geöffnet.

3. Wählen Sie in der Drop-down-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".



Das Dialogfeld "ARCserve VMware-Konfigurationstool" wird geöffnet.

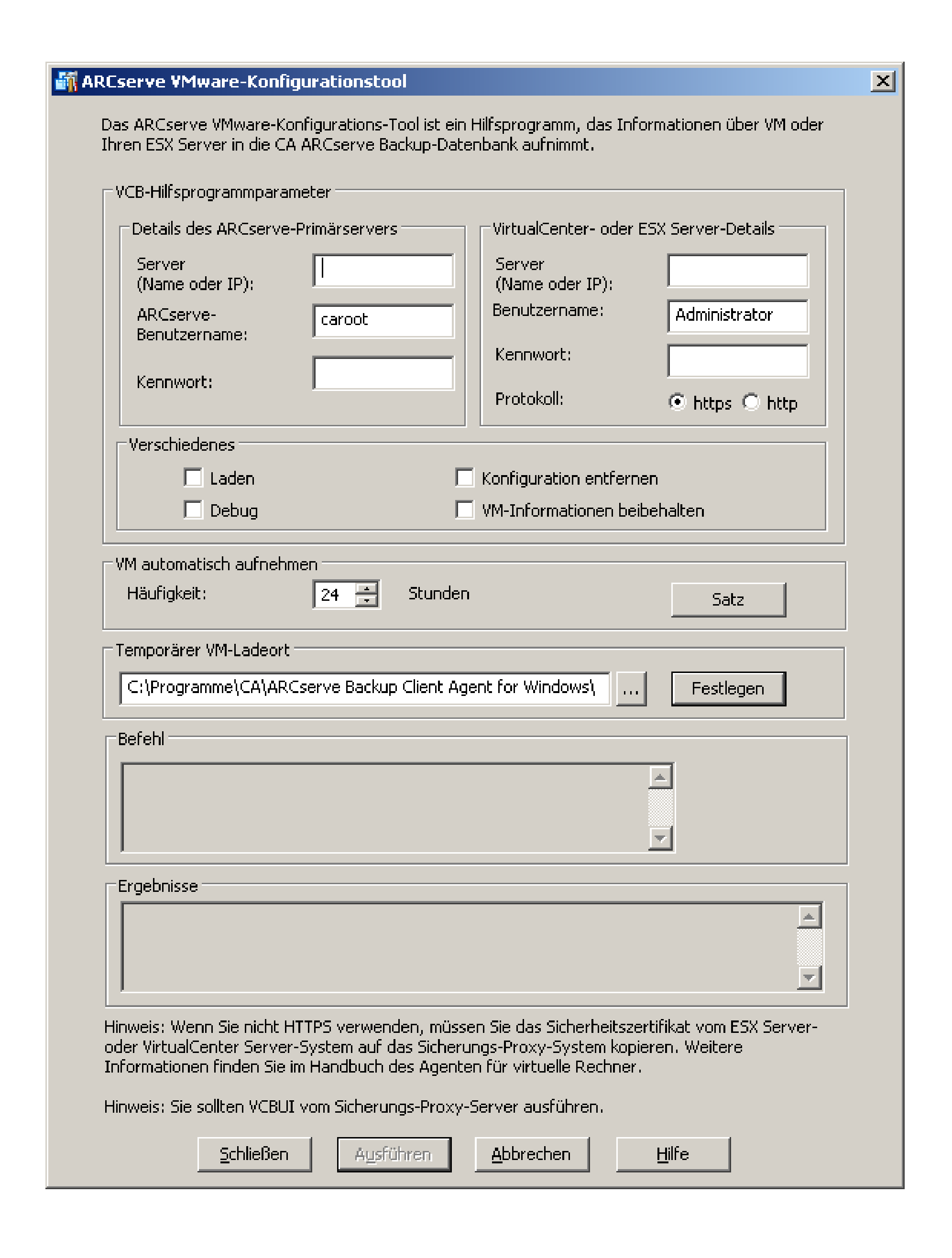
Hinweis: (Optional) Sie können "VCBUI.exe" in den folgenden Verzeichnissen auf dem Sicherungs-Proxy-System öffnen:

- X86-Systeme

  `C:\Programme\CA\ARCserve Backup Client Agent for Windows`

- x64-Systeme

  `C:\Programme\CA\ARCserve Backup Client Agent für Windows\x86`


ARCserve VMware-Konfigurationstool
Das ARCserve VMware-Konfigurations-Tool ist ein Hilfsprogramm, das Informationen über VM oder Ihren ESX Server in die CA ARCserve Backup-Datenbank aufnimmt.
VCB-Hilfsprogrammparameter
Details des ARCserve-Primärservers
Server (Name oder IP):
ARCserve-Benutzername:
caroot
Kennwort:
VirtualCenter- oder ESX Server-Details
Server (Name oder IP):
Benutzername:
Administrator
Kennwort:
Protokoll:
https
http
Verschiedenes
Laden
Debug
Konfiguration entfernen
VM-Informationen beibehalten
VM automatisch aufnehmen
Häufigkeit:
24
Stunden
Satz
Temporärer VM-Ladeort
C:\Programme\CA\ARCserve Backup Client Agent for Windows\
Festlegen
Befehl
Ergebnisse
Hinweis: Wenn Sie nicht HTTPS verwenden, müssen Sie das Sicherheitszertifikat vom ESX Server- oder VirtualCenter Server-System auf das Sicherungs-Proxy-System kopieren. Weitere Informationen finden Sie im Handbuch des Agenten für virtuelle Rechner.
Hinweis: Sie sollten VCBUI vom Sicherungs-Proxy-Server ausführen.
Schließen
Ausführen
Abbrechen
Hilfe

4. Füllen Sie die folgenden Felder im Dialogfeld "ARCserve VMware-Konfigurationstool" aus:

   Informationen zum ARCserve-Primärserver

   Folgende Optionen gelten für den Primärserver oder für den eigenständigen Server von CA ARCserve Backup:

   - **Server (Name oder IP):** Hier können Sie den Namen oder die IP-Adresse des CA ARCserve Backup-Primärsystems angeben.
   - **ARCserve-Benutzername:** Hier können Sie den Benutzernamen (mit Caroot-Rechten) für das CA ARCserve Backup-Primärsystem angeben.
   - **Kennwort:** Hier können Sie das Kennwort für den CA ARCserve Backup-Benutzernamen eingeben.

   vCenter Server- oder VMware ESX Host-Details

   Folgende Optionen gelten für die virtuelle VMware-Infrastruktur in Ihrer Umgebung:

   - **Server (Name oder IP):** Hier können Sie den Namen des VMware ESX Host- oder vCenter Server-Systems angeben.
   - **Benutzername:** Hier können Sie den Namen des VMware ESX Host oder vCenter-Benutzers (mit Administratorrechten) angeben.
   - **Kennwort:** Ermöglicht die Eingabe des Kennworts für den VMware ESX Host-Benutzernamen oder den vCenter Server-Benutzernamen.
   - **Protokoll:** Hier können Sie das Protokoll für die Kommunikation zwischen dem Sicherungs-Proxy-System und dem VMware ESX Host-System oder vCenter Server-System angeben.

     Hinweis: Falls Sie dieses Argument auslassen, verwendet das Tool https als Kommunikationsprotokoll.

Verschiedenes

Legen Sie die folgenden verschiedenen Optionen nach Bedarf fest, um Informationen in die CA ARCserve Backup-Datenbank einzupflegen:

- **Laden:** Wenn die Option "Laden" aktiviert ist, pflegt das Konfigurationstool die Namen der VMs, die geladen werden können, in die Datenbank ein.

  Hinweis: Wenn Sie das Konfigurationstool ausführen und die Option "Laden" nicht aktiviert ist, dauert das Ausführen des Hilfsprogramms länger, da für jede ausgeführte VM ein Lade- und ein Entladevorgang ausgeführt wird.

- **Konfiguration entfernen:** Ermöglicht das Löschen der in der Datenbank verfügbaren VMs für das angegebene VMware ESX Host- oder vCenter Server-System für ein angegebenes Sicherungs-Proxy-System.

- **Debug:** Mit dieser Option können Sie ein detailliertes Debug-Protokoll schreiben. Das Protokoll wird im Client Agent für Windows-Installationsverzeichnis erstellt. Dieses Verzeichnis lautet standardmäßig wie folgt:

  ```
  C:\Programme\CA\ARCserve Backup Client Agent for Windows\LOG
  ```

  Hinweis: Der Name der Protokolldatei lautet "ca_vcbpopulatedb.log".

- **VM-Informationen beibehalten**: Ermöglicht Ihnen, Daten (Sicherungsinformationen) für virtuelle Rechner, die nicht verfügbar sind, wenn Sie dieses Tool ausführen, beizubehalten.

  Standardmäßig erfasst dieses Tool Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Tool ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

  Berücksichtigen Sie die folgenden Hinweise zu optimalen Verfahren:

  - Aktivieren Sie die Option zum Beibehalten der VM-Informationen in Umgebungen, in denen die VMs während des Auffüllungsvorgangs nicht ausgeführt werden. Durch diese Vorgehensweise stellen Sie sicher, dass CA ARCserve Backup beim nächsten Ausführen des Sicherungsjobs die VMs sichert.
  - Deaktivieren Sie die Option zum Beibehalten der VM-Informationen in Umgebungen, in denen die virtuellen Rechner von einem ESX-Server- oder vCenter Serversystem zu einem anderen migriert werden, um Lastverteilungsvorgänge zu unterstützen. Diese Vorgehensweise hilft dabei, sicherzustellen, dass Sicherungen von ESX-Server- und vCenter Serversystemen nicht fehlschlagen.

- **Automatisches Auffüllen beenden:** Ermöglicht, dass CA ARCserve Backup das automatische Laden der VM-bezogenen Informationen für das ESX Server- oder vCenter Server-System beendet.

  Als Best Practice wird die Verwendung dieser Option in den folgenden Szenarien empfohlen:

  - Die CA ARCserve Backup-Datenbank wurde mit Informationen über die ESX Server- oder vCenter Server-Systeme gefüllt. Sie wollen jetzt den automatischen CA ARCserve Backup-Datenbankauffüllungsprozess stoppen.
  - Ein ESX Server- oder vCenter Server-System wurde deaktiviert. Nachdem das System wieder gestartet worden war, wurde die CA ARCserve Backup-Datenbank mit Informationen über das ESX Server- oder vCenter Server-System aufgefüllt. Sie wollen jetzt den automatischen CA ARCserve Backup-Datenbankauffüllungsprozess stoppen.
  - Ein neues ESX Server- oder vCenter Server-System wurde in Ihrer Sicherungsumgebung installiert. Die CA ARCserve Backup-Datenbank wurde mit Informationen über das ESX Server- oder vCenter Server-System aufgefüllt. Sie wollen jetzt den automatischen CA ARCserve Backup-Datenbankauffüllungsprozess stoppen.

  Wenn die Option "Automatische Auffüllung beenden" aktiviert ist, wird der automatische Datenbankauffüllungsprozess das nächste Mal, wenn CA ARCserve Backup die CA ARCserve Backup-Datenbank auffüllen soll, nicht ausgeführt. Der automatische Datenbankauffüllungsprozess füllt die Datenbank nach abgeschlossenem Sicherungsjob in 24-stündigen Intervallen (Standardeinstellung) oder basierend auf der Häufigkeit, die Sie für diese Option festgelegt haben, mit aktualisierten Informationen auf.

VM automatisch auffüllen

Hiermit können Sie festlegen, wie oft die CA ARCserve Backup-Datenbank automatisch mit Informationen zu virtuellen Rechnern gefüllt wird.

Standardeinstellung: 24 Stunden

Bereich: 1 bis 99 Stunden

Temporärer VM-Ladeort

Legt fest, wo das ARCserve VMware-Konfigurationstool während dessen Ausführung die Sicherungsinformationen für die VMs vorübergehend lädt (speichert).

Standardmäßig speichert CA ARCserve Backup die temporären Sicherungsinformationen am folgenden Speicherort:

```
C:\Programme\CA\ARCserve Backup Client Agent for Windows
```

Hinweis: Sie müssen auf "Festlegen" klicken, um den Speicherort zu übernehmen.

Es kann beispielsweise nötig sein, den temporären Ladeort zu verschieben, da nicht genügend freier Speicherplatz vorhanden ist, um die Sicherung auf das Volume zu laden. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

5. Klicken Sie auf "Execute".

   Hinweis: Sie können erst dann auf "Ausführen" klicken, wenn alle erforderlichen Felder vollständig ausgefüllt sind.

   Das ARCserve VMware-Konfigurationstool füllt die CA ARCserve Backup-Datenbank auf. Die Ergebnisse der Ausführung werden im Feld "Ergebnisse" des ARCserve VMware-Konfigurationstools angezeigt. Zum Anzeigen detaillierter Protokollinformationen öffnen Sie die Protokolldatei mit dem Namen "ca_vcbpopulatedb.log", die sich im Installationsverzeichnis des Client Agent für Windows auf dem Sicherungs-Proxysystem befindet.

Einpflegen von Informationen in die Datenbank mithilfe des ARCserve-Konfigurationstools für Hyper-V

Das ARCserve Hyper-V-Konfigurationstool ist ein Hilfsprogramm zum Sammeln von Daten, das Informationen zu den VMs im Hyper-V-Hostsystem in die CA ARCserve Backup-Datenbank einpflegt.

Nach der Installation des Agenten müssen Sie die CA ARCserve Backup-Datenbank mit Informationen zu Ihren VM-Systemen füllen. Hierfür müssen Sie das ARCserve Hyper-V-Konfigurationstool auf dem Hyper-V-Hostsystem ausführen.

Nachdem Sie das ARCserve-Hyper-V-Konfigurationstool ausgeführt und einen Sicherungsjob für die Daten auf den virtuellen Rechnern übergeben haben, wird die CA ARCserve Backup-Datenbank automatisch mit den Informationen über die virtuellen Rechner aufgefüllt, die bei der Ausführung des Konfigurationstools angegeben wurden. Mit der Option für das automatische Auffüllen können Sie sicherstellen, dass der Sicherungs-Manager richtig durchsucht wird und die aktuellen Daten auf den virtuellen Rechnern gesichert werden. CA ARCserve Backup füllt die Datenbank standardmäßig automatisch in 24-Stunden-Abständen nach Abschluss der Sicherung mit aktualisierten Daten.

Beachten Sie beim ARCserve Hyper-V-Konfigurationstool folgende Einschränkungen:

- Informationen zu virtuellen Hyper-V-Rechnern, die zum Zeitpunkt der Ausführung dieses Tools heruntergefahren waren, werden vom ARCserve-Hyper-V-Konfigurationstool in die CA ARCserve Backup-Datenbank aufgenommen. Das Tool kann die Datenbank nicht mit Daten von virtuellen Hyper-V-Rechnern auffüllen, wenn die VMs ausgeschaltet sind.
- Das ARCserve-Hyper-V-Konfigurationstool füllt die CA ARCserve Backup-Datenbank mit den Hostnamen der ermittelten VMs auf. Falls das ARCserve-Hyper-V-Konfigurationstool den Hostnamen eines virtuellen Rechners nicht ermitteln kann, ersetzt CA ARCserve Backup den Hostnamen der VM mit dem VM-Namen der VM in der CA ARCserve Backup-Datenbank.
- CA ARCserve Backup unterstützt nur Hostnamen und VM-Namen, die maximal 15 Zeichen umfassen. Wenn die ermittelten Hostnamen oder VM-Namen länger als 15 Zeichen sind, werden sie in der CA ARCserve Backup-Datenbank auf 15 Zeichen gekürzt.
- Das ARCserve-Hyper-V-Konfigurationstool unterstützt die Verwendung von JIS2004-Unicode-Zeichen für Hostnamen und VM-Namen nicht. Wenn das Tool JIS2004-Unicode-Zeichen in den Namen erkennt, erfasst CA ARCserve Backup dieses Ereignis im Feld "Ergebnis" im ARCserve-Hyper-V-Konfigurationstool, und die Informationen zu den VMs werden nicht in die CA ARCserve Backup-Datenbank aufgenommen.

So pflegen Sie Informationen in die Datenbank mithilfe des ARCserve-Konfigurationstools für Hyper-V ein

1. Stellen Sie sicher, dass die VMs in Ihren Hyper-V-Serversystemen laufen.

   Hinweis: Das ARCserve-Hyper-V-Konfigurationstool füllt die CA ARCserve Backup-Datenbank nicht mit Information zu virtuellen Hyper-V-Rechner aus, die nicht laufen.

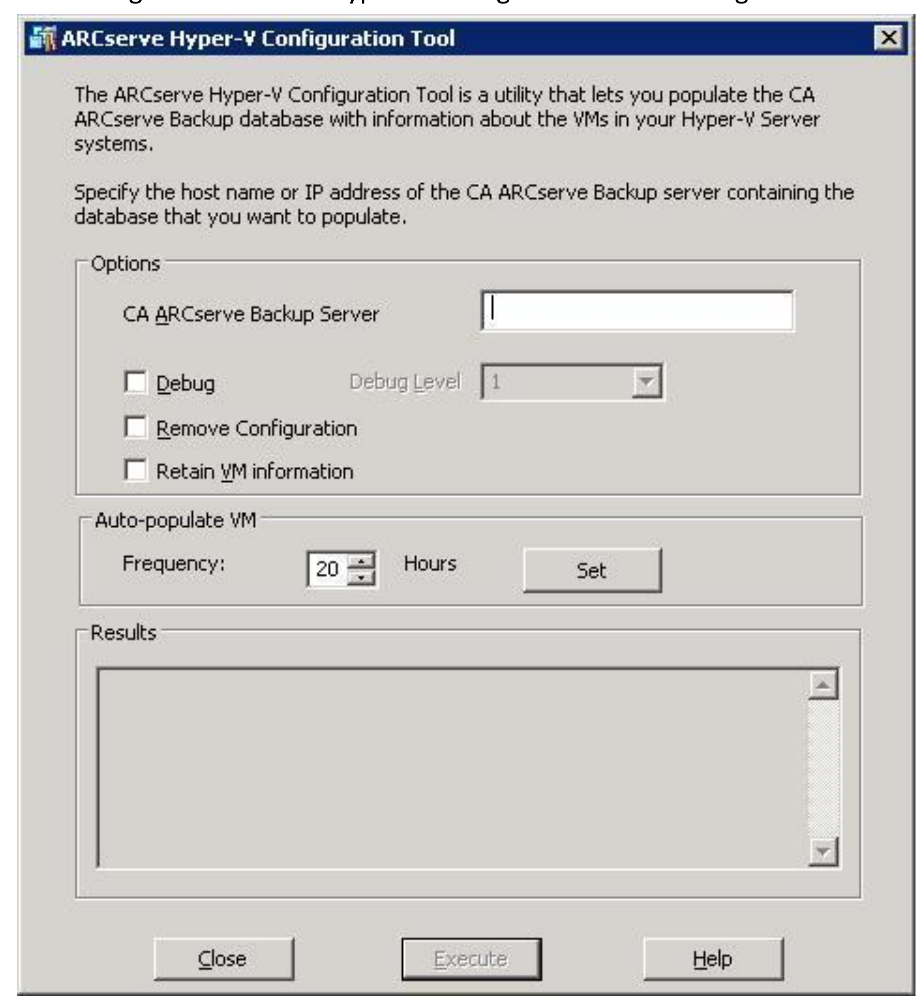
2. Melden Sie sich beim Hyper-V-Hostsystem an, und öffnen Sie die Backup Agent-Verwaltung.

   Sie finden die Backup Agent-Verwaltung unter "Start", "Programme", "CA", "ARCserve Backup", "Backup Agent – Verwaltung".

   Das Dialogfeld "Backup Agent - Verwaltung" wird geöffnet.

3. Wählen Sie in der Drop-down-Liste die Option "CA ARCserve Backup Agent für virtuelle Rechner", und klicken Sie in der Symbolleiste auf die Schaltfläche "Konfiguration".

   Das Dialogfeld "ARCserve-Hyper-V-Konfigurationstool" wird geöffnet.



4. Füllen Sie die folgenden Felder im Dialogfeld "ARCserve-Hyper-V-Konfigurationstool" aus:

   Optionen

   - **CA ARCserve Backup-Server:** Hier können Sie den Hostnamen oder die IP-Adresse des CA ARCserve Backup-Servers angeben, der die zu füllende Datenbank enthält.
   - **Debug:** Mit dieser Option können Sie ein detailliertes Debug-Protokoll schreiben. Das Protokoll wird im Client Agent für Windows-Installationsverzeichnis erstellt. Dieses Verzeichnis lautet standardmäßig wie folgt:

     ```
     C:\Programme\CA\ARCserve Backup Client Agent für Windows\Log
     ```

     Hinweis: Der Name der Protokolldatei lautet "ca_msvmpopulatedb.log".
   - **Debug-Ebene:** Hier geben Sie die gewünschte Detailgenauigkeit für das Debug-Protokoll an ("ca_msvmpopulatedb.log").

     Standardeinstellung: 2

     Bereich: 1 bis 6.

     Hinweis: Eine höhere Debug-Ebene bedeutet, dass detailliertere Informationen im Debug-Protokoll angegeben werden.

- **Konfiguration entfernen**: Hiermit können Sie die virtuellen Rechner löschen, die in der CA ARCserve Backup-Datenbank für den angegebenen Hyper-V-Server verfügbar sind.
- **VM-Informationen beibehalten**: Ermöglicht Ihnen, Daten (Sicherungsinformationen) für virtuelle Rechner, die nicht verfügbar sind, wenn Sie dieses Tool ausführen, beizubehalten.

  Standardmäßig erfasst dieses Tool Informationen von virtuellen Rechnern, die verfügbar sind, wenn Sie dieses Tool ausführen. Wenn eine VM nicht verfügbar ist (zum Beispiel weil sie heruntergefahren oder aus der Umgebung gelöscht wurde), löscht CA ARCserve Backup die mit dieser VM verbundenen Daten aus der CA ARCserve Backup-Datenbank. Wenn diese Option aktiviert wurde, erfasst CA ARCserve Backup Informationen zu virtuellen Rechnern, die verfügbar sind, und behält die Sicherungsinformationen von virtuellen Rechnern, die nicht verfügbar sind, bei.

  Berücksichtigen Sie die folgenden Hinweise zu optimalen Verfahren:

  - Aktivieren Sie die Option zum Beibehalten der VM-Informationen in Umgebungen, in denen die VMs während des Auffüllungsvorgangs nicht ausgeführt werden. Durch diese Vorgehensweise stellen Sie sicher, dass CA ARCserve Backup beim nächsten Ausführen des Sicherungsjobs die VMs sichert.
  - Deaktivieren Sie die Option zum Beibehalten der VM-Informationen in Umgebungen, in denen die VMs von einem Hyper-V-Server zu einem anderen migrieren, um Lastverteilungsvorgänge zu unterstützen. Durch diese Vorgehensweise stellen Sie sicher, dass Sicherungen, die vom Hyper-V-Server ausgeführt werden, nicht fehlschlagen.

VM automatisch aufnehmen

- **Häufigkeit:** Hiermit können Sie festlegen, wie oft die CA ARCserve Backup-Datenbank automatisch mit Informationen zu virtuellen Rechnern aufgefüllt wird.

  Standardeinstellung: 24 Stunden

  Bereich: 1 bis 99 Stunden

  Hinweis: Sie müssen auf "Festlegen" klicken, um den Wert für Häufigkeit zu übernehmen.

5. Klicken Sie auf "Execute".

   Die CA ARCserve Backup-Datenbank wird mit Informationen über die VMs gefüllt, die im Hyper-V-Hostsystem ausgeführt werden.

Auffüllen der CA ARCserve Backup-Datenbank mithilfe von Befehlszeilenhilfsprogrammen

Mit CA ARCserve Backup können Sie die folgenden Befehlszeilenhilfsprogramme verwenden, um die CA ARCserve Backup-Datenbank aufzufüllen:

- **ca_vcbpopulatedb:** Ermöglicht das Auffüllen der CA ARCserve Backup-Datenbank mit Informationen über die VMware-VMs in Ihrer Sicherungsumgebung.
- **ca_msvmpopulatedb:** Ermöglicht as Auffüllen der CA ARCserve Backup-Datenbank mit Informationen über Hyper-V-VMs in Ihrer Sicherungsumgebung.

Hinweis: Weitere Informationen über die Syntax, Argumente und Beispiele für die oben beschriebenen Hilfsprogramme finden Sie im *Befehlszeilen-Referenzhandbuch*.

Auswirkung der VM-Namen auf Jobs

CA ARCserve Backup unterscheidet virtuelle Rechner anhand ihrer VM-Namen (DNS-Namen) in Verbindung mit ihren Hostnamen oder dem Namen des Sicherungs-Proxy-Systems. CA ARCserve Backup füllt die CA ARCserve Backup-Datenbank mit diesen Informationen, wenn Sie das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool ausführen.

Mithilfe des ARCserve VMware-Konfigurationstools und des ARCserve Hyper-V-Konfigurationstools können Sie Informationen zu den virtuellen Rechnern in der CA ARCserve Backup-Datenbank beibehalten oder entfernen, indem Sie die Option "VM-Informationen beibehalten" entweder aktivieren oder deaktivieren. Mithilfe dieses Designs können Sie Informationen zu den ausgeschalteten virtuellen Rechnern beibehalten, wenn Sie die oben genannten Tools ausführen.

Das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool greifen auf den VM-Namen zurück, um den Status eines virtuellen Rechners zu bestimmen (Beispiel: der VM ist ausgeschaltet). Wenn das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool nicht in der Lage sind, einen virtuellen Rechner anhand seines VM-Namens zu finden, suchen die Tools virtuelle Rechner anhand von deren Hostnamen oder anhand des Namens des Sicherungs-Proxy-Systems.

Beispiel: Auswirkungen von VM-Namen auf Jobs

Stellen Sie sich folgende VM-Umgebung vor:

- Sie erstellen eine Umgebung, die aus einem virtuellen Rechner besteht.
- Der Hostname dieses VM lautet VM1.
- Der VM-Name ist "VM_eins".

Folgende Ereignisse finden statt:

1. Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus.

   CA ARCserve Backup füllt die CA ARCserve Backup-Datenbank mit den Informationen zu den Daten, die auf VM1 vorhanden sind.

2. Sie übergeben einen geplanten Sicherungsjob von VM1.

   CA ARCserve Backup führt den Job aus und dieser wird erfolgreich abgeschlossen.

3. Sie benennen VM1 in VM2 um, Sie ändern jedoch nicht den VM-Namen.
4. Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus und aktivieren die Option "VM-Informationen beibehalten".

   CA ARCserve Backup füllt die Datenbank mit Informationen zu den Daten, die auf VM2 vorhanden sind.

   Hinweis: Bei den Sicherungsdaten zu VM2 handelt es sich um die Daten, die sich auf VM_eins befinden.

5. Sie übergeben einen geplanten Sicherungsjob von VM2 und schalten diesen anschließend aus.
6. CA ARCserve Backup führt beide Jobs aus. Dabei kommen folgende Ergebnisse zustande:

   - Die Sicherung von VM1 wird erfolgreich abgeschlossen. Die Sicherungsdaten bestehen aus den Daten, die sich auf VM2 befinden.
   - Die Sicherung von VM2 wird erfolgreich abgeschlossen. Die Sicherungsdaten bestehen aus den Daten, die sich auf VM2 befinden.

Beobachtungen:

- In diesem Beispiel hat der Benutzer den Hostnamen des VM geändert, jedoch nicht den VM-Namen.
- CA ARCserve Backupist nicht in der Lage, einen virtuellen Rechner anhand seines Hostnamens zu finden (zum Beispiel VM1 und VM2), wenn der virtuelle Rechner ausgeschaltet ist. In diesem Szenario sucht CA ARCserve Backup nach dem VM-Namen (zum Beispiel VM_eins), der dem Hostnamen entspricht.
- Wenn beide virtuellen Rechner ausgeschaltet sind, haben sie in der CA ARCserve Backup-Datenbank dieselbe Identität. Infolgedessen sichert CA ARCserve Backup während der Ausführung des VM1-Jobs den falschen virtuellen Rechner.

Kapitel 4: Sichern von Daten

Dieses Kapitel enthält folgende Themen:

So durchsuchen Sie VM-Sicherungsdatenträger

Im Sicherungs-Manager können Sie innerhalb einer Verzeichnisstruktur Informationen zu folgenden VM-Objekten durchsuchen und anzeigen:

- Sicherungs-Proxysysteme
- VMware ESX/ESXi Server-Systeme
- VMware vCenter Server-Systeme
- Microsoft Hyper-V-Hostsysteme

Damit Sie VMware-VMs und Hyper-V-VMs durchsuchen können, müssen Sie das ARCserve VMware-Konfigurationstool und das ARCserve Hyper-V-Konfigurationstool ausführen. Diese Tools füllen die CA ARCserve Backup-Datenbank mit Informationen zu den in den VMs enthaltenen Daten, sodass Sie die VMs im Sicherungs-Manager durchsuchen können.

Beachten Sie folgende Einschränkungen:

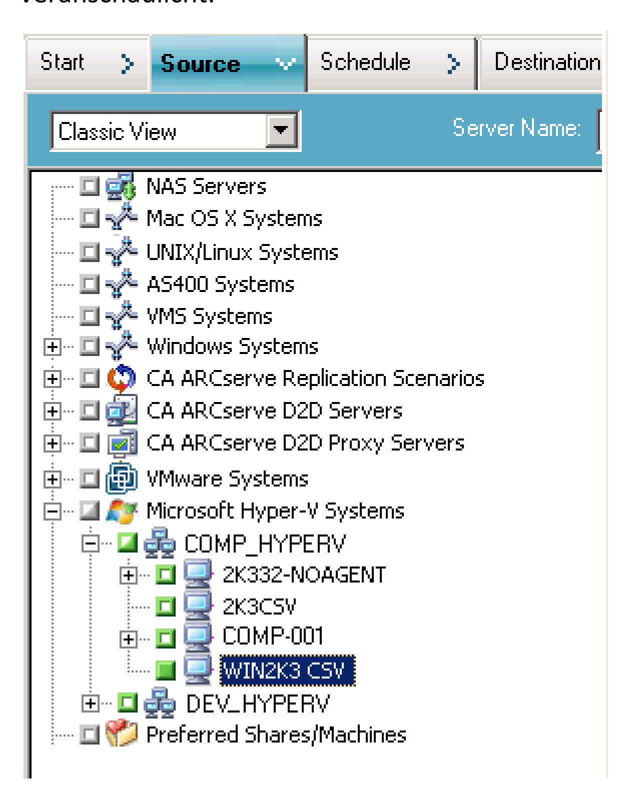
- Sie können die Volumes der VMware-VMs durchsuchen, wenn die VM ein VMware-unterstütztes, Windows-basiertes Betriebssystem ausführt.
- Sie können die Volumes in den Hyper-V-VMs durchsuchen, wenn Sie den Agent für virtuelle Rechner auf den Hyper-V-VMs installieren. Bei dieser Konfiguration ist es nicht erforderlich, das ARCserve Hyper-V-Konfigurationstool auszuführen, um die Volumes der Hyper-V-VMs zu durchsuchen.

- Wenn im Sicherungs-Manager die Registerkarte "Quelle" ausgewählt ist, kann das Objekt "VMware-Systeme" eingeblendet werden, sodass die Namen der VMware-Systeme, der Sicherungs-Proxy-Systeme, des ESX Server-Systems oder des vCenter Server-Systems sowie die im Windows-Betriebssystem enthaltenen VM-Volumes angezeigt werden. Auf VM-Ebene können Sie im Raw-Modus (vollständige VM) oder im Dateimodus durchsuchen.

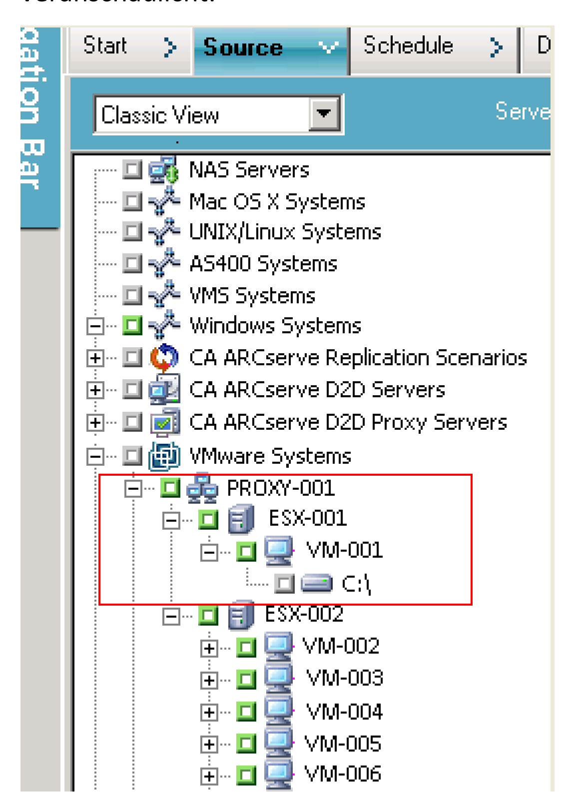
  Um eine VM auf Dateiebene zu durchsuchen, muss ein VMware-unterstütztes Windows-Betriebssystem auf der VM installiert sein.

- Durchsuchungsmodi:
  - Windows VMs: Dateimodus und Raw-Modus (vollständige VM).
  - VMs, die von anderen Systemen als Windows unterstützt werden: Nur Raw-Modus (vollständige VM).

Im folgenden Bildschirm wird das Durchsuchen von Hyper-V-VMs veranschaulicht:



Im folgenden Bildschirm wird das Durchsuchen von VMware-VMs veranschaulicht:



- Wenn Sie einen Sicherungsjob übergeben, werden Sie von CA ARCserve Backup dazu aufgefordert, die Benutzernamen- und Kennwortinformationen für das ESX Server-, das vCenter Server- oder das Hyper-V Host-System anzugeben.

  CA ARCserve Backup überprüft die Anmeldeinformationen während der Laufzeit.

Sicherungsmethoden

Bevor Sie einen Sicherungsjob übergeben, müssen Sie die Methode angeben, die Sie für Ihre Sicherungen verwenden wollen. Sie können VCB oder VDDK angeben. Als Best Practice empfiehlt sich die VDDK-Methode.

Hinweis: Weitere Informationen über die Vorteile, die das Verwenden der VDDK-Methode bietet, finden Sie unter Einführung zur Integration in VMware vSphere (siehe Seite 21).

Informationen über die VDDK-Methode, die VCB-Methode und das Festlegen einer Sicherungsmethode finden Sie unter Festlegen von Sicherungsmethoden (siehe Seite 51).

Globale und lokale Sicherungsoptionen

Dieser Abschnitt enthält folgende Themen:

Funktionsweise von globalen und lokalen Sicherungsoptionen

Die Sicherungsoptionen bestimmen, wie CA ARCserve Backup auf VMs gespeicherte Daten sichert. In CA ARCserve Backup können Sie Sicherungsdaten mit folgenden Sicherungsoptionen verarbeiten:

- **Dateimodus:** Damit können Sie auf VMs gespeicherte einzelne Dateien oder Verzeichnisse sichern. Bei Sicherungen im Dateimodus können Sie VM-Sicherungsdaten mit Dateiebenengranularität wiederherstellen.

  Standardmäßig wird in CA ARCserve Backup VCB-Framework zum Durchführen von Sicherungen auf Dateiebene verwendet, wenn VCB-Framework und VDDK auf dem Sicherungs-Proxy-System installiert sind. Falls auf dem Sicherungs-Proxy-System jedoch nur VDDK installiert ist, wird in CA ARCserve Backup VDDK zum Durchführen von Sicherungen auf Dateiebene von VM-Daten verwendet. VMware VDDK unterstützt das Durchsuchen von Volume-Bereitstellungspunkten nicht, die sich auf Sicherungen auf Dateiebene beziehen.

- **Raw-Modus (vollständige VM):** Hiermit können Sie ein vollständiges Image der auf einer VM befindlichen Daten sichern. Im Raw-Modus (vollständige VM) können Sie Daten sichern, die für Disaster Recovery-Vorgänge verwendet werden können.

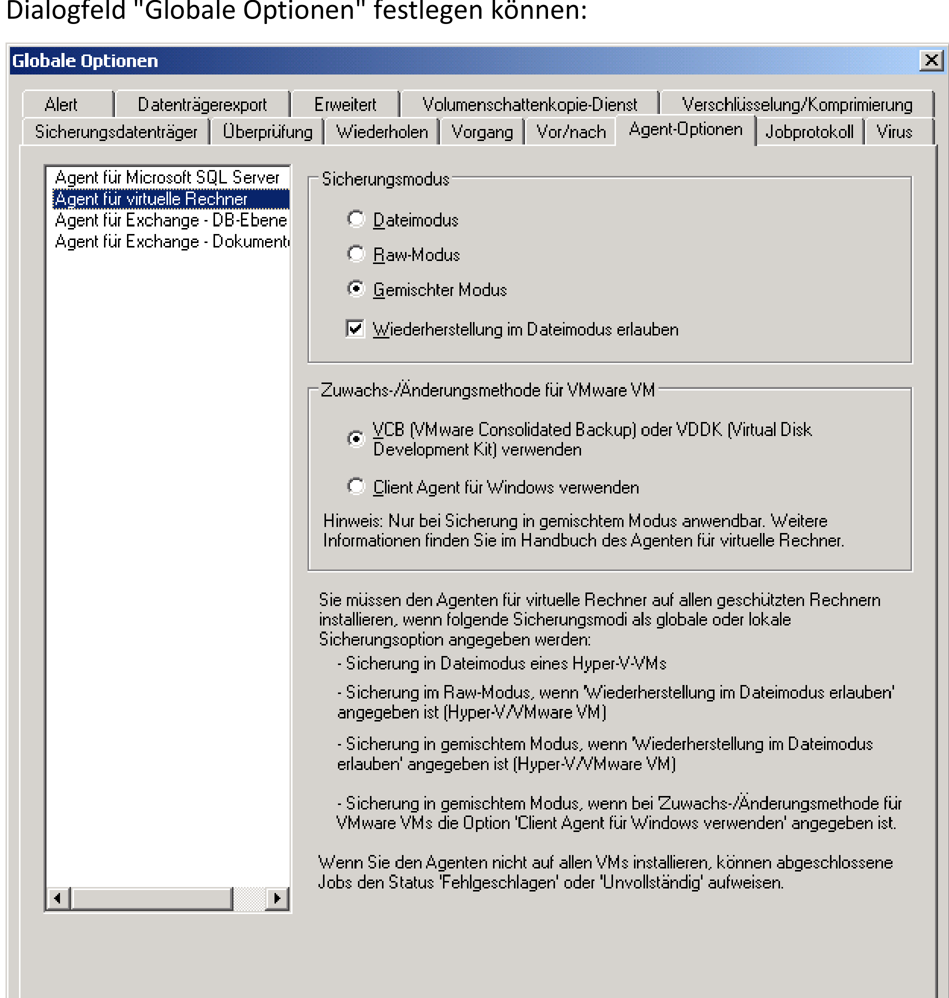
- **Gemischter Modus:** Ermöglicht das Durchführen vollständiger Datensicherungen im Raw-Modus (vollständige VM) sowie von Zuwachs- und Änderungssicherungen im Dateimodus. Mit Sicherungen im gemischten Modus können Sie geplante Sicherungen und GFS-Rotationssicherungen durchführen. Außerdem bieten Sicherungen im gemischten Modus den Vorteil, dass sie wöchentliche, vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen mit Dateiebenengranularität durchführen können.

  Hinweis: Die Standardeinstellung bilden Sicherungen im gemischten Modus.

- **Wiederherstellung im Dateimodus erlauben**: Mit dieser Option können Sie Raw-(vollständige VM-)Sicherungen und Sicherungen im gemischten Modus auf Dateiebenengranularität wiederherstellen.

  Hinweis: Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter Angeben des CA ARCserve Backup-Servernamens (siehe Seite 69).

Im folgenden Dialogfeld werden die VM-Sicherungsmodi dargestellt, die Sie im Dialogfeld "Globale Optionen" festlegen können:



Sie können Sicherungsmodi entweder als globale Sicherungsoption oder als lokale Sicherungsoption festlegen.

- **Globale Sicherungsoption:** Damit werden Sicherungsmodi global auf alle Sicherungsjobs angewendet, die sich auf VMs in VMware- und Hyper-V-Systemen in Ihrer Umgebung beziehen. Weitere Informationen finden Sie im Abschnitt zum Festlegen von Sicherungsmodi als globale Sicherungsoption (siehe Seite 100).
- **Lokale Sicherungsoption:** Damit können Sie auf Jobebene einen Sicherungsmodus auf einzelne VMware- und Hyper-V-VMs anwenden. Weitere Informationen finden Sie unter Festlegen von Sicherungsmodi als lokale Sicherungsoption (siehe Seite 103).

Hinweis: Wenn Sie Sicherungsmodi auf globaler und lokaler Ebene festlegen, führt CA ARCserve Backup den Sicherungsjob immer mit den lokalen Sicherungsoptionen aus, die für die betreffende VM festgelegt wurden.

In der folgenden Tabelle wird das Verhalten der Sicherungsmodi beschrieben:

Ausgewählter Sicherungsmodus	Ausgewählte globale Änderungs- /Zuwachsmethode	Ergebnis unter VMware-Systemen	Ergebnis unter Hyper-V-Systemen
Gemischt (als globale oder lokale Option ausgewählt)	■ Verwenden von VCB oder VDDK	CA ARCserve Backup verarbeitet die Daten der Raw-Sicherung (vollständige VM-Sicherung) und die Daten von Sicherungen im Dateimodus (Zuwachs- und Änderungssicherungen) mithilfe von VCB oder VDDK. **Hinweis:** Bei Sicherungen im gemischten Modus verarbeitet CA ARCserve Backup die Raw-Sicherung mithilfe des angegebenen Modus: VCB oder VDDK. Allerdings werden Sicherungen im Dateimodus von CA ARCserve Backup immer mithilfe von VCB verarbeitet, wenn VCB und VDDK auf dem Sicherungs-Proxy-System installiert sind.	CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus unter Verwendung des VSS-Hyper-V Writers und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Agenten für virtuelle Rechner, der auf der VM ausgeführt wird. **Hinweis:** Die globale Option zur Verwendung von VCB/VDDK wirkt sich nicht auf Sicherungen auf Hyper-V-Systemen aus.

Ausgewählter Sicherungsmodus	Ausgewählte globale Änderungs-/Zuwachsmethode	Ergebnis unter VMware-Systemen	Ergebnis unter Hyper-V-Systemen
Gemischt (als globale oder lokale Option ausgewählt)	■ Client Agent verwenden **Hinweis:** Der Agent für virtuelle Rechner muss auf der VM installiert sein und ausgeführt werden.	CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus unter Verwendung von VCB/VDDK und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Client Agent für Windows, der auf der VM ausgeführt wird.	CA ARCserve Backup verarbeitet die wöchentlichen vollständigen Sicherungen im Raw-Modus (vollständige VM) unter Verwendung des VSS-Hyper-V Writers und die aufeinander folgenden täglichen Zuwachs- und Änderungssicherungen im Dateimodus unter Verwendung des Agenten für virtuelle Rechner, der auf den VMs ausgeführt wird. **Hinweis:** Die globale Option zur Verwendung von VCB/VDDK wirkt sich nicht auf Sicherungen auf Hyper-V-Systemen aus.

Beispiele: So wenden Sie Sicherungsoptionen an

Um Daten im Raw-Modus (vollständige VM-Sicherung) sichern und mit Dateiebenengranularität wiederherstellen zu können, empfiehlt sich als Best Practice, die Standardoptionen für den Sicherungsmodus zu übernehmen und global auf alle Sicherungen anzuwenden. Um eine einzelne VM zu schützen, etwa eine VM, auf der ein unterstütztes Nicht-Windows-Betriebssystem ausgeführt wird, können Sie die Sicherungsoptionen entweder für die einzelne VM festlegen; oder Sie können sie als lokale Sicherungsoption festlegen und dann die global für alle Sicherungen ausgewählten Optionen beibehalten.

Ihre Sicherungsumgebung besteht aus zahlreichen Servern, auf denen VMs installiert sind. Die meisten Ihrer Sicherungen sind Rotationssicherung für VMs. Die übrigen Server erfordern vollständige Sicherungen im dateibasierten Modus. Um den Konfigurationsprozess zu vereinfachen, können Sie die Sicherung im gemischten Modus global auf alle Sicherungen anwenden und dann den Sicherungsmodus auf Dateiebene lokal auf alle Server anwenden, auf denen Sie Sicherungen auf Dateiebene ausführen möchten.

Festlegen von Sicherungsmodi als globale Sicherungsoption

Globale Optionen betreffen alle VM-Sicherungen auf Jobebene in Ihrer Umgebung. Legen Sie mit den folgenden Schritten Sicherungsmodi fest, die für alle VM-Sicherungsjobs gelten.

So legen Sie Sicherungsmodi als globale Sicherungsoption fest:

1. Öffnen Sie den Sicherungs-Manager, und klicken Sie auf die Registerkarte "Quelle".

   Die Quellverzeichnisstruktur wird angezeigt.

2. Erweitern Sie das Objekt "VMware-Systeme" oder das Objekt "Microsoft Hyper-V-Systeme", und navigieren Sie zu der zu sichernden VM.

   Klicken Sie in der Symbolleiste auf "Optionen".

   Das Dialogfeld "Optionen" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Agent-Optionen" und dann auf "Agent für virtuelle Rechner".

4. Geben Sie einen Sicherungsmodus an, indem Sie auf eine der folgenden Optionen klicken:

   - **Dateimodus:** Ermöglicht Ihnen, einzelne Dateien und Verzeichnisse zu schützen. Mit Sicherungen im Dateimodus können Sie folgende Aufgaben ausführen:

     – In einer VM enthaltene Dateien und Verzeichnisse auf Dateiebenengranularität sichern

     – Vollständige Sicherungen, Zuwachs- und Änderungssicherungen durchführen

     – Daten auf Dateiebenengranularität wiederherstellen

     – Mehrere Daten-Streams mithilfe der Multistreaming-Option gleichzeitig bearbeiten

     – Daten mithilfe der Filteroption filtern

     Hinweis: Die erforderliche Laufzeit für die Sicherung einer vollständigen VM auf Dateiebene ist länger als die erforderliche Laufzeit für die Sicherung desselben Volumes auf Raw-Ebene (vollständige VM).

   - **Raw-Modus:** Ermöglicht Ihnen, ganze Systeme für Disaster Recovery zu schützen. Mit Sicherungen im Raw-Modus können Sie folgende Aufgaben ausführen:

     – Ausschließlich Durchführen vollständiger Sicherungen von vollständigen VM-Images

     – Mehrere Daten-Streams mithilfe der Multistreaming-Option gleichzeitig bearbeiten

     Hinweis: Im Raw-Modus können Daten nicht auf Dateiebenengranularität wiederhergestellt oder Raw-Daten (vollständige VM) gefiltert werden. Bei Sicherungen im Raw-Modus (vollständige VM) angewendete Filter werden während der Laufzeit ignoriert.

- **Gemischter Modus:** Die Standardsicherungsmethode ist der gemischte Modus. Im gemischten Modus können Sie folgende Aufgaben ausführen:

  - GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen

  Hinweis: Rotations- und GFS-Rotationsjobs haben den Vorteil, dass Sie Sicherungsdaten enthalten, die Ihnen den täglichen Schutz (Sicherungen auf Dateiebene) und den Disaster Recovery-Schutz (vollständige VM-Sicherungen im Raw-Modus) in einem einzigen Sicherungsjob bieten.

- **Wiederherstellung im Dateimodus erlauben:** Damit können Sie Daten mit der Effizienz des Raw-Modus sichern und Daten mit Dateiebenengranularität wiederherstellen. Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter Angeben des CA ARCserve Backup-Servernamens (siehe Seite 69).

  Mit der Option zum Aktivieren der Wiederherstellung auf Dateiebene können Sie folgende Aufgaben ausführen:

  - Daten aus Raw-Modus-Sicherungen (vollständiges VM) auf Dateiebenengranularität wiederherstellen
  - Daten aus Sicherungen im gemischten Modus auf Dateiebenengranularität wiederherstellen

  Mit der Option "Wiederherstellung auf Dateiebene erlauben" zeigt CA ARCserve Backup das folgende Verhalten:

  - Die Option "Wiederherstellung auf Dateiebene erlauben" können Sie für alle Sicherungstypen verwenden, einschließlich benutzerdefinierte Sicherungen, Rotationssicherungen und GFS-Rotationen, die aus vollständigen Sicherungen, Zuwachssicherungen und Änderungssicherungen bestehen. Die vollständigen Sicherungen werden im Raw-Modus erstellt (vollständige VM), und die Zuwachs- und Änderungssicherungen werden im Sicherungsmodus auf Dateiebene erstellt. Wenn Sie die Aktivierung der Wiederherstellung auf Dateiebene nicht festlegen, stellt CA ARCserve Backup nur die Zuwachs- und Änderungssicherungen wieder her. Die im Raw-Modus erstellte vollständige Sicherung wird bei der Wiederherstellung nicht mit einbezogen.

- **Zuwachs-/Änderungssicherungsmethode für VMware-VM:** Hiermit können Sie die Kommunikationsmethode angeben, die CA ARCserve Backup zur Übertragung von Daten der Zuwachs- und Änderungssicherung zwischen VMware-VMs und dem Sicherungs-Proxy-System verwendet.
  - **VCB/VDDK verwenden:** Diese Option legt fest, dass CA ARCserve Backup VMware Virtual Consolidated Backup verwendet, um Daten der Zuwachs- bzw. Änderungssicherung an das Sicherungs-Proxy-System zu übermitteln. Sie sollten diese Option aktivieren, um die Belastung Ihres Netzwerks zu reduzieren.

    Hinweis: Die Option "VCB/VDDK verwenden" ist standardmäßig aktiviert.
  - **Client Agent für Windows verwenden:** Sorgt dafür, dass CA ARCserve Backup zur Ausführung der Sicherung Client Agent für Windows verwendet. Mit dieser Option führt CA ARCserve Backup eine Dateisystemsicherung durch, bei der das Sicherungs-Proxysystem nicht für den Abschluss der Sicherung erforderlich ist.

Klicken Sie auf "OK".

Der Sicherungsmodus wird auf alle Ihre VM-Sicherungen angewendet.

5. Klicken Sie auf "OK", um das Dialogfeld "Optionen" zu schließen.

Festlegen von Sicherungsmodi als lokale Sicherungsoption

Lokale Optionen wirken sich auf einzelne VM-Sicherungen auf der Jobebene aus. Legen Sie mit den folgenden Schritten Sicherungsmodi fest, die für einzelne Sicherungsjobs gelten.

So legen Sie Sicherungsmodi als lokale Sicherungsoption fest:

1. Öffnen Sie den Sicherungs-Manager, und klicken Sie auf die Registerkarte "Quelle".

   Die Quellverzeichnisstruktur wird angezeigt.

2. Erweitern Sie das Objekt "VMware-Systeme" oder das Objekt "Microsoft Hyper-V-Systeme", und navigieren Sie zu der zu sichernden VM.

   Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Lokale Optionen" aus.

   Das Dialogfeld "Sicherungsmodus" wird geöffnet.

3. Klicken Sie auf "Globale Optionen außer Kraft setzen". Weitere Informationen finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

   Geben Sie einen Sicherungsmodus an, indem Sie auf eine der folgenden Optionen klicken:

   - **Dateimodus:** Ermöglicht Ihnen, einzelne Dateien und Verzeichnisse zu schützen. Mit Sicherungen im Dateimodus können Sie folgende Aufgaben ausführen:
     - In einer VM enthaltene Dateien und Verzeichnisse auf Dateiebenengranularität sichern
     - Vollständige Sicherungen, Zuwachs- und Änderungssicherungen durchführen
     - Daten auf Dateiebenengranularität wiederherstellen
     - Mehrere Daten-Streams mithilfe der Multistreaming-Option gleichzeitig bearbeiten
     - Daten mithilfe der Filteroption filtern

     Hinweis: Die erforderliche Laufzeit für die Sicherung einer vollständigen VM auf Dateiebene ist länger als die erforderliche Laufzeit für die Sicherung desselben Volumes auf Raw-Ebene (vollständige VM).

   - **Raw-Modus:** Ermöglicht Ihnen, ganze Systeme für Disaster Recovery zu schützen. Mit Sicherungen im Raw-Modus können Sie folgende Aufgaben ausführen:
     - Ausschließlich Durchführen vollständiger Sicherungen von vollständigen VM-Images
     - Mehrere Daten-Streams mithilfe der Multistreaming-Option gleichzeitig bearbeiten

     Hinweis: Im Raw-Modus können Daten nicht auf Dateiebenengranularität wiederhergestellt oder Raw-Daten (vollständige VM) gefiltert werden. Bei Sicherungen im Raw-Modus (vollständige VM) angewendete Filter werden während der Laufzeit ignoriert.

- **Gemischter Modus:** Die Standardsicherungsmethode ist der gemischte Modus. Im gemischten Modus können Sie folgende Aufgaben ausführen:

  - GFS- und Rotationssicherungsjobs durchführen, die wöchentliche vollständige Sicherungen im Raw-Modus (vollständige VM) und tägliche Zuwachs- und Änderungssicherungen im Dateimodus in einem einzigen Sicherungsjob umfassen

  Hinweis: Rotations- und GFS-Rotationsjobs haben den Vorteil, dass Sie Sicherungsdaten enthalten, die Ihnen den täglichen Schutz (Sicherungen auf Dateiebene) und den Disaster Recovery-Schutz (vollständige VM-Sicherungen im Raw-Modus) in einem einzigen Sicherungsjob bieten.

- **Wiederherstellung im Dateimodus erlauben:** Damit können Sie Daten mit der Effizienz des Raw-Modus sichern und Daten mit Dateiebenengranularität wiederherstellen. Um Wiederherstellungen auf Dateiebenengranularität von Raw-(vollständigen VM-)Sicherungen durchführen zu können, müssen Sie den Namen des CA ARCserve Backup-Servers auf Ihren virtuellen Rechnern angeben. Weitere Informationen finden Sie unter Angeben des CA ARCserve Backup-Servernamens (siehe Seite 69).

  Mit der Option zum Aktivieren der Wiederherstellung auf Dateiebene können Sie folgende Aufgaben ausführen:

  - Daten aus Raw-Modus-Sicherungen (vollständiges VM) auf Dateiebenengranularität wiederherstellen
  - Daten aus Sicherungen im gemischten Modus auf Dateiebenengranularität wiederherstellen

  Mit der Option "Wiederherstellung auf Dateiebene erlauben" zeigt CA ARCserve Backup das folgende Verhalten:

  - Die Option "Wiederherstellung auf Dateiebene erlauben" können Sie für alle Sicherungstypen verwenden, einschließlich benutzerdefinierte Sicherungen, Rotationssicherungen und GFS-Rotationen, die aus vollständigen Sicherungen, Zuwachssicherungen und Änderungssicherungen bestehen. Die vollständigen Sicherungen werden im Raw-Modus erstellt (vollständige VM), und die Zuwachs- und Änderungssicherungen werden im Sicherungsmodus auf Dateiebene erstellt. Wenn Sie die Aktivierung der Wiederherstellung auf Dateiebene nicht festlegen, stellt CA ARCserve Backup nur die Zuwachs- und Änderungssicherungen wieder her. Die im Raw-Modus erstellte vollständige Sicherung wird bei der Wiederherstellung nicht mit einbezogen.

Klicken Sie auf "OK".

Das Dialogfeld "Sicherungsmodus" wird geschlossen, und der Sicherungsmodus wird angewendet.

Verarbeitung von Zuwachs- und Änderungssicherungen virtueller VMware-Rechner durch den Agenten

Der Agent verwendet folgende Dateieigenschaften als Datei-Auswahlkriterien für Zuwachs- und Änderungssicherungen:

- **Erstellungs- oder Änderungsdatum der Datei:** Sicherungen der VCB-Kommunikation

  Der Agent kommuniziert über VCB mit dem virtuellen Rechner. Der Agent ermittelt und filtert Daten basierend auf dem Erstellungs- oder Änderungszeitpunkt der Dateien. Mithilfe dieser Kommunikationsmethode sichert der Agent unabhängig von Datei-Attributen alle Dateien mit Erstellungs- oder Änderungszeitpunkten, die sich zeitlich vor der letzten vollständigen Sicherung oder -Zuwachssicherung befinden.

- **Archivbit:** Client Agent für Windows-Kommunikationssicherungen

  Der Agent kommuniziert über den Client Agent für Windows mit dem virtuellen Rechner. Der Agent ermittelt und filtert Dateien basierend auf dem Archivbit. Wenn der Agent Systemstatusdateien und Dateien mit dem Status "FilesNotToBackup" ermittelt, schließt er diese von der Zuwachs- oder Änderungssicherung aus.

Hinweis: Weitere Informationen zur Sicherungsoption "VCB verwenden" und den Kommunikationssicherungen "Client Agent für Windows verwenden" finden Sie unter Festlegen von Sicherungsmodi als globale Sicherungsoption (siehe Seite 100).

Sichern von Daten auf VMware-VMs

Mit CA ARCserve Backup können Sie Daten sichern, die sich auf VMware-VMs befinden. Befolgen Sie die nachstehenden Schritte, um Sicherungsjobs auf lokalen, festplattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs zu übergeben.

Hinweis: Weitere Informationen zu den Einschränkungen bei Sicherungen mit VCB finden Sie unter "Einschränkungen beim Sichern und Wiederherstellen mit VCB (siehe Seite 30)".

So sichern Sie Daten auf VMware-VMs

1. Öffnen Sie das Fenster "Sicherungs-Manager", und wählen Sie die Registerkarte "Quelle" aus.

   Die Quellverzeichnisstruktur des Sicherungs-Managers wird angezeigt.

2. Blenden Sie das Objekt "VMware-Systeme" ein.

   Die Sicherungs-Proxy-Systeme, VMware ESX Host-Systeme, vCenter Server-Systeme und VMs in Ihrer Umgebung werden angezeigt.

3. Aktivieren Sie das Kontrollkästchen neben den Objekten, die gesichert werden sollen. Sie können Volumes, einen kompletten Knoten oder eine Kombination davon als Quelle auswählen.

   Hinweis: Informationen zum Durchsuchen von Datenträgern finden Sie im Abschnitt So durchsuchen Sie VM-Sicherungsdatenträger. (siehe Seite 91)

4. Legen Sie einen Sicherungsmodus für den Job fest.

   Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

5. Um VM-Sicherungsdaten zu filtern, klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Filter" aus.

   Hinweis: Weitere Informationen zu Filtern finden Sie unter "Filtern von VM-Sicherungsdaten (siehe Seite 115)".

   Wichtig! Wenn der "Sicherungsmodus" auf "Raw-Modus" festgelegt ist und Sie Filter angeben, filtert CA ARCserve Backup keine VM-Sicherungsdaten.

6. Um anzugeben, wo Sie den Sicherungsjob speichern möchten, klicken Sie auf die Registerkarte "Ziel" oder die Registerkarte "Staging".

   Hinweis: Weitere Informationen zur Zielfestlegung oder zum Staging bei der Datensicherung finden Sie im *Administrationshandbuch*.

   Zur Verwendung von Multistreaming bei der Übermittlung von Sicherungsdaten aktivieren Sie das Kontrollkästchen "Multi-Stream".

7. Um die Planungsoptionen für den Job anzugeben, klicken Sie auf die Registerkarte "Ablaufplan".

   Hinweis: Weitere Informationen zu den Optionen der Jobplanung finden Sie im *Administrationshandbuch*.

8. Um globale Filter anzugeben, klicken Sie in der Symbolleiste auf "Filter".

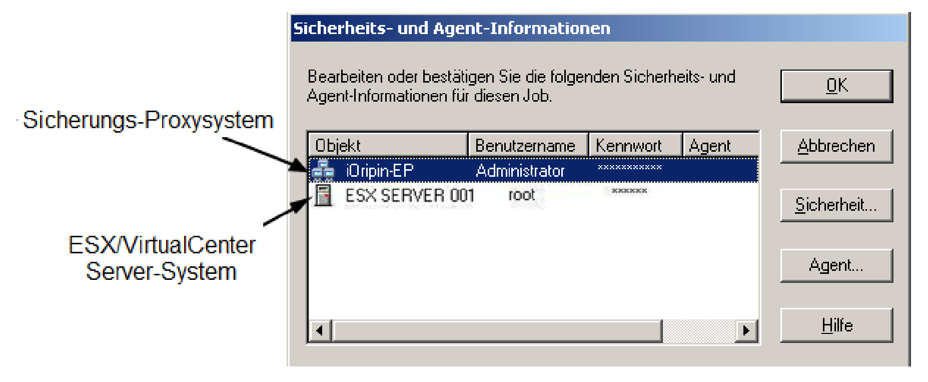
   Das Dialogfeld "Filter" wird geöffnet.

   Hinweis: Weitere Informationen zum Filtern von VM-Daten finden Sie unter "Filtern von VM-Sicherungsdaten (siehe Seite 115)". Wenn Sie weitere Informationen zum Angeben von Filtern benötigen, klicken Sie im Dialogfeld "Filter" auf die Schaltfläche "Hilfe".

9. Klicken Sie auf der Symbolleiste auf die Sendeschaltfläche, um den Job zu senden.

   Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet.

   Sie müssen die Anmeldeinformationen für das VMware ESX Host- oder vCenter Server-System und das Sicherungs-Proxy-System eingeben, um den Job zu übergeben.



10. Wählen Sie den zu sichernden Server aus, und klicken Sie im Dialogfeld "Sicherheits- und Agent-Informationen" auf die Schaltfläche "Sicherheit".

    Das Dialogfeld "Sicherheit" wird angezeigt.

11. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

    Hinweis: CA ARCserve Backup unterstützt nur Systemanmeldungen mit Kennwörtern, die maximal 23 Zeichen umfassen. Wenn das Kennwort für das System, bei dem Sie sich anmelden möchten, mehr als 23 Zeichen umfasst, müssen Sie das Kennwort auf dem Agenten-System so ändern, dass es höchstens 23 Zeichen aufweist, damit Sie sich beim Agenten-System anmelden können.

    CA ARCserve Backup wendet Ihre Sicherheitsinformationen an, und das Dialogfeld "Job übergeben" wird geöffnet.

12. Nehmen Sie im Dialogfeld "Job übergeben" Eingaben in den erforderlichen Feldern vor, und klicken Sie auf "OK".

    Hinweis: Klicken Sie im Dialogfeld "Job übergeben" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen.

    CA ARCserve Backup übergibt den Job. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch*.

So benennt der Agent Bereitstellungspunkte

CA ARCserve Backup verwendet für jeden Typ von VM-Sicherung eine andere Namenskonvention für Bereitstellungspunkte.

Für VCB Framework-Sicherungen verwendet CA ARCserve Backup die folgende Namenskonvention:

- Wenn eine VCB-Sicherung ausgeführt wird, erstellt CA ARCserve Backup ein Bereitstellungspunkt-Verzeichnis (Snapshot) auf dem Sicherungs-Proxy-System. In CA ARCserve Backup wird der Snapshot mit der folgenden Regel benannt:

  `_VCB-BACKUP_`

- Nach Abschluss der Sicherung löscht CA ARCserve Backup den VM-Snapshot vom Sicherungs-Proxy-System. Wenn die Sicherung nicht erfolgreich abgeschlossen wird, bleibt der Snapshot auf dem Sicherungs-Proxy-System erhalten, bis der nächste Sicherungsjob gestartet und der Snapshot gelöscht wird. Nachfolgende Sicherungen schlagen fehl, wenn der Snapshot in CA ARCserve Backup nicht vom Sicherungs-Proxy-System gelöscht werden kann.

Für VDDK-Sicherungen wird in CA ARCserve Backup die folgende Namenskonvention verwendet:

- Wenn eine VDDK-Sicherung ausgeführt wird, erstellt CA ARCserve Backup ein Bereitstellungspunkt-Verzeichnis (Snapshot) auf dem Sicherungs-Proxy-System. In CA ARCserve Backup wird der Snapshot mit der folgenden Regel benannt:

  ```
  _ARCServe_Backup__ J<JobID>_S<SessionID>_Datum_Uhrzeit
  ```

- Nach Abschluss der Sicherung wird der Snapshot in CA ARCserve Backup vom Sicherungs-Proxy-System gelöscht. Wenn die Sicherung nicht erfolgreich abgeschlossen wird, bleibt der Snapshot auf dem Sicherungs-Proxy-System erhalten, bis Sie ihn vom ESX Server-System löschen. Snapshots, die auf dem Sicherungs-Proxy-System verbleiben, haben keine Auswirkungen auf nachfolgende Sicherungen.

Sichern von Daten auf Hyper-V-VMs

Gehen Sie wie im Folgenden beschrieben vor, um Sicherungsjobs auf lokalen, plattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs zu übergeben.

Hinweis: Weitere Informationen zu den Einschränkungen bei Sicherungen mit VCB finden Sie unter "Einschränkungen beim Sichern und Wiederherstellen mit VCB (siehe Seite 30)".

So sichern Sie Daten auf Hyper-V-VMs

1. Öffnen Sie das Fenster "Sicherungs-Manager", und wählen Sie die Registerkarte "Quelle" aus.

   Die Quellverzeichnisstruktur des Sicherungs-Managers wird angezeigt.

2. Blenden Sie das Objekt "Microsoft Hyper-V-Systeme" ein.

   Die Hyper-V-Systeme in Ihrer Umgebung werden angezeigt.

3. Aktivieren Sie das Kontrollkästchen neben den Objekten, die gesichert werden sollen. Sie können Volumes, einen kompletten Knoten oder eine Kombination davon als Quelle auswählen.

   Hinweis: Informationen zum Durchsuchen von Datenträgern finden Sie im Abschnitt So durchsuchen Sie VM-Sicherungsdatenträger. (siehe Seite 91)

4. Legen Sie einen Sicherungsmodus für den Job fest.

   Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

5. Um VM-Sicherungsdaten zu filtern, klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Filter" aus.

   Hinweis: Weitere Informationen zu Filtern finden Sie unter "Filtern von VM-Sicherungsdaten (siehe Seite 115)".

   Wichtig! Wenn der "Sicherungsmodus" auf "Raw-Modus" festgelegt ist und Sie Filter angeben, filtert CA ARCserve Backup keine VM-Sicherungsdaten.

6. Um anzugeben, wo Sie den Sicherungsjob speichern möchten, klicken Sie auf die Registerkarte "Ziel" oder die Registerkarte "Staging".

   Hinweis: Weitere Informationen zur Zielfestlegung oder zum Staging bei der Datensicherung finden Sie im *Administrationshandbuch*.

   Zur Verwendung von Multistreaming bei der Übermittlung von Sicherungsdaten aktivieren Sie das Kontrollkästchen "Multi-Stream".

7. Um die Planungsoptionen für den Job anzugeben, klicken Sie auf die Registerkarte "Ablaufplan".

   Hinweis: Weitere Informationen zu den Optionen der Jobplanung finden Sie im *Administrationshandbuch*.

8. Um globale Filter anzugeben, klicken Sie in der Symbolleiste auf "Filter".

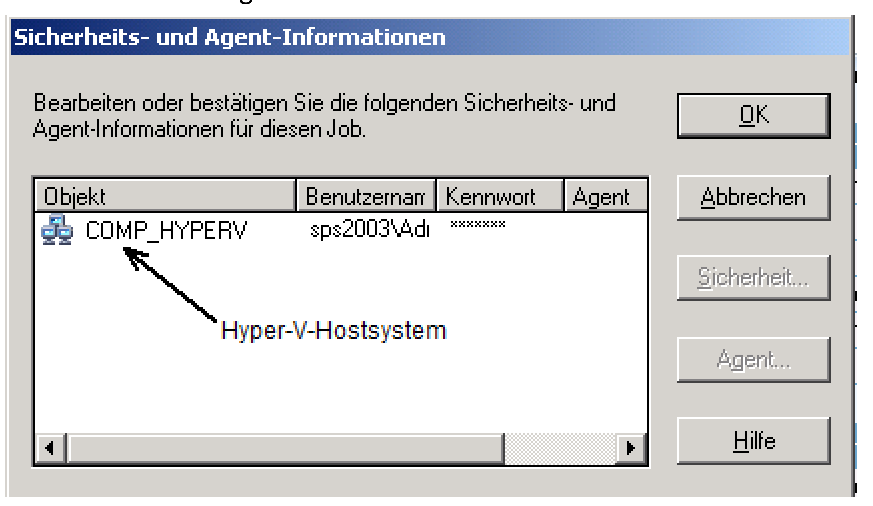
   Das Dialogfeld "Filter" wird geöffnet.

   Hinweis: Weitere Informationen zum Filtern von VM-Daten finden Sie unter "Filtern von VM-Sicherungsdaten (siehe Seite 115)". Wenn Sie weitere Informationen zum Angeben von Filtern benötigen, klicken Sie im Dialogfeld "Filter" auf die Schaltfläche "Hilfe".

9. Klicken Sie auf der Symbolleiste auf die Sendeschaltfläche, um den Job zu senden.

   Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet.

   Sie müssen Anmeldeinformationen für das Hyper-V-Hostsystem angeben, um den Job zu übergeben.



10. Wählen Sie den zu sichernden Server aus, und klicken Sie im Dialogfeld "Sicherheits- und Agent-Informationen" auf die Schaltfläche "Sicherheit".

    Das Dialogfeld "Sicherheit" wird angezeigt.

11. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

    Hinweis: CA ARCserve Backup unterstützt nur Systemanmeldungen mit Kennwörtern, die maximal 23 Zeichen umfassen. Wenn das Kennwort für das System, bei dem Sie sich anmelden möchten, mehr als 23 Zeichen umfasst, müssen Sie das Kennwort auf dem Agenten-System so ändern, dass es höchstens 23 Zeichen aufweist, damit Sie sich beim Agenten-System anmelden können.

    CA ARCserve Backup wendet Ihre Sicherheitsinformationen an, und das Dialogfeld "Job übergeben" wird geöffnet.

12. Nehmen Sie im Dialogfeld "Job übergeben" Eingaben in den erforderlichen Feldern vor, und klicken Sie auf "OK".

    Hinweis: Klicken Sie im Dialogfeld "Job übergeben" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen.

    CA ARCserve Backup übergibt den Job. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch*.

Verschiedene Tasks

Dieser Abschnitt enthält folgende Themen:

Funktionsweise der Agent-Unterstützung für das Hilfsprogramm Preflight-Check

Mit dem Hilfsprogramm Preflight-Check (PFC) können Sie wichtige Überprüfungen auf dem CA ARCserve Backup-Server und den zugehörigen Agenten ausführen, so dass Sie die möglichen Ursachen für das Fehlschlagen von Sicherungsjobs erkennen können.

Bei Sicherungen von virtuellen Rechnern überprüft das PFC-Hilfsprogramm den Status des Client Agent für Windows, der auf dem Sicherungs-Proxysystem bzw. dem Hyper-V-Hostsystem ausgeführt wird. PFC überprüft nicht den Status der VMs, die Sie für die Sicherung auf dem VMware ESX Host- oder vCenter Server-System angegeben haben.

Hinweis: Weitere Informationen zur Verwendung des PFC-Hilfsprogramms finden Sie im "*Administrationshandbuch*".

Mit dem PFC-Hilfsprogramm werden folgende Überprüfungen für VMware ESX Host-Sicherungen in folgenden Szenarien durchgeführt:

- Mit dem Agenten wird ein Sicherungsjob übergeben. Der Client Agent für Windows wird auf dem Sicherungs-Proxy-System ausgeführt.

  Die folgende Meldung wird angezeigt:

  ```
  Hinweis: Der Zielknoten <Name/IP des Proxysystems> ist ein VMware-
  Proxysystem. PFC überprüft den Status des Client Agent auf dem VMware-Proxy-
  Server. Der Status der virtuellen Rechner (VMs), die Sie auf dem VMware ESX-
  Server zur Sicherung ausgewählt haben, wird nicht überprüft.
  ```

- Mit dem Agenten wird ein Sicherungsjob übergeben. Der Client Agent für Windows wird auf dem Sicherungs-Proxy-System nicht ausgeführt.

  Die folgende Meldung wird angezeigt:

  ```
  Probleme: Verbindung zum Client Agent auf <Name/IP des Proxy-Systems> konnte
  nicht hergestellt werden. Stellen Sie sicher, dass der Client Agent auf
  <Name/IP des Proxy-Systems> ausgeführt wird.
  Hinweis: Der Zielknoten <Name/IP des Proxysystems> ist ein VMware-
  Proxysystem. PFC überprüft den Status des Client Agent auf dem VMware-Proxy-
  Server. Der Status der virtuellen Rechner (VMs), die Sie auf dem VMware ESX-
  Server zur Sicherung ausgewählt haben, wird nicht überprüft.
  ```

Filtern von VM-Sicherungsdaten

In CA ARCserve Backup können Sie Daten filtern, wenn Sie eine Sicherung im Dateimodus oder eine Rotationsicherung im gemischten Modus durchführen, die Zuwachssicherungen und/oder Änderungssicherungen umfasst. Mit dieser Funktion können Sie folgende Aufgaben ausführen:

- Sicherung der Daten auf der VMs basierend auf beispielsweise Dateimuster, Datumsbereich, Änderungsdatum, Dateigröße usw.
- Sicherung von ausgewählten Dateien, Ordnern oder beidem in einem ausgewählten Volume
- Anwendung von globalen oder lokalen Filterkriterien auf Ihre Sicherungsjobs

  Hinweis: Ein *globaler* Filter wendet Filter auf all Ihre Sicherungsjobs an, während ein *lokaler* Filter lediglich Filter auf die ausgewählte VM anwendet.

So filtern Sie VM-Sicherungsdaten:

1. Öffnen Sie den Sicherungs-Manager, und suchen Sie nach der VM, die Sie filtern möchten.
2. Führen Sie eine der folgenden Aktionen aus:
   - Zur Anwendung von globalen Filtern bei Ihrer Sicherung klicken Sie in der Symbolleiste des Sicherungs-Managers auf die Schaltfläche "Filter".
   - Zur Anwendung von lokalen Filtern bei Ihrer Sicherung klicken Sie mit der rechten Maustaste auf das VM-Objekt, und wählen Sie im Kontextmenü "Filter" aus.

   Das Dialogfeld "Filter" wird geöffnet.
3. Geben Sie die Filter an, die zum Abschließen des Sicherungsjobs erforderlich sind.

   Hinweis: Informationen zur Datenfilterung erhalten Sie, wenn Sie im Dialogfeld "Filter" auf "Hilfe" klicken.

Protokolldateien des Agenten

CA ARCserve Backup beinhaltet Protokolldateien, die Ihnen Einzelheiten zu Sicherungsvorgängen liefern, die mithilfe des Agenten für virtuelle Rechner ausgeführt wurden. CA ARCserve Backup speichert die Protokolldateien auf dem Sicherungs-Proxy-System und dem Hyper-V-Hostsystem an folgendem Speicherort:

```
C:\Programme\CA\ARCserve Backup Client Agent für Windows\Log
```

Folgende Protokolldateien gelten für Sicherungen von VMware-VMs:

recovervm.log

Zeigt Informationen zu Wiederherstellungsvorgängen aus "VM wiederherstellen" an.

ca_vcbpopulatedb.log

Zeigt Meldungen zu Sicherungsjobs von VMware-VMs an.

Die Meldungen beginnen mit der Job-ID und der Sitzungsnummer, durch die Sie Jobs unterscheiden können, die gleichzeitig ausgeführt werden.

- **Maximale Protokollgröße**: Standardmäßig beschränkt der Agent die Größe von "ca_vcbpopulatedb.log" auf 250 KB. Um die Grenze zu ändern (zu erhöhen oder zu verringern), erstellen Sie folgende Registrierung:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe
  Backup\ClientAgent\Parameters\VMMaxLogSize
  ```

  Wertdaten: Legen Sie die maximale Protokollgröße fest, die Sie benötigen.

mount_jnl.log

Zeigt Informationen zu Lade- und Entladevorgängen an.

Die Protokolldatei enthält die für jeden Lade- und Entladevorgang angegebenen Parameter.

ca_vcbmounteroutput_xxx.log

Zeigt Informationen zu fehlgeschlagenen Lade- und Entladevorgängen an.

- **Maximale Protokollanzahl**: Standardmäßig speichert CA ARCserve Backup maximal 1 000 Protokolldateien. Sie können eine andere Anzahl an Protokolldateien festlegen, indem Sie die Wertdaten in folgendem Registrierungsschlüssel ändern:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe
  Backup\ClientAgent\Parameters\VMMaxLogFiles
  ```

  Hinweis: Wenn die Anzahl der "ca_vcbmounteroutput_xxx.log"-Protokolle den maximalen Wert erreicht, überschreibt CA ARCserve Backup "ca_vcbmounteroutput_000.log" beim nächsten Ladevorgang und löscht "ca_vcbmounteroutput_001.log".

- **Maximale Protokollgröße**: Standardmäßig beschränkt der Agent die Größe der Datei "ca_vcbmounteroutput_xxx.log" auf 250 KB. Um die Grenze zu ändern (zu erhöhen oder zu verringern), erstellen Sie folgende Registrierung:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe
  Backup\ClientAgent\Parameters\VMMaxMountLogSize
  ```

  Wertdaten: Legen Sie die maximale Protokollgröße fest, die Sie benötigen.

Die folgende Protokolldatei gilt für Sicherungen von Hyper-V-VMs:

Hyper.log

Zeigt Meldungen zu Sicherungen und Wiederherstellungen von Hyper-V-VMs an.

Die Meldungen beginnen mit der Job-ID und der Sitzungsnummer, durch die Sie Jobs unterscheiden können, die gleichzeitig ausgeführt werden.

Die folgende Protokolldatei gilt für Sicherungen von VMware- und Hyper-V-VMs:

vmdbupd.log

Enthält Informationen zur automatischen Aufnahme.

Die Protokolldatei enthält die angegebenen Parameter und den Status aller automatischen Ausführungen des ARCserve VMware-Konfigurationstools (siehe Seite 73) und des ARCserve Hyper-V-Konfigurationstools (siehe Seite 82).

Schutz von Volumes, die von virtuellen Festplatten aus bereitgestellt wurden

Dieser Abschnitt enthält folgende Themen:

Übersicht über virtuelle Festplatten

Eine virtuelle Festplatte (VHD) ist ein Image-Format, das dank verschiedener Virtualisierungsmethoden den Inhalt einer Festplatte und virtuelle Betriebssysteme sowie deren zugeordnete Anwendungen in einer einzelnen Datei enthält. Sie können daher VHD-Dateien (.vhd), die sich in Container-Volumes befinden, zur Ausführung von Betriebssystemen von virtuellen Rechnern aus verwenden. Container-Volumes können unter anderem eine Sammlung von Betriebssystemdateien, Datendateien und Treibern enthalten, wodurch das Betriebssystem in der VHD-Funktion unabhängig von der VHD, in der es enthalten ist, bereitgestellt wird.

CA ARCserve Backup schützt die in VHDs geladenen Volumen.

Beschränkungen beim Schutz von Volumen, die von virtuellen Festplatten bereitgestellt werden

Beachten Sie folgende Einschränkungen bei der Sicherung von VHDs:

- Daten können mit CA ARCserve Backup nicht auf Dateiebenengranularität wiederhergestellt werden, wenn Sie VHD-Volumes sichern, die im VM bereitgestellt wurden.

  Beachten Sie Folgendes:

  - Hinweis: Diese Beschränkung gilt nur, wenn im Raw-Sicherungsmodus (vollständige VM-Sicherung) die Option "Wiederherstellung im Dateimodus erlauben" aktiviert wird.
  - Diese Beschränkung bezieht sich nicht auf Sicherungen, die mithilfe von Client Agent für Windows ausgeführt werden. CA ARCserve Backup kann keine Daten mit Dateiebenengranularität wiederherstellen, wenn nur Client Agent für Windows verwendet wird.

- CA ARCserve Backup unterstützt die Verwendung von VSS zur Sicherung von geschachtelten VHD-Volumes nicht für mehr als eine Datenebene.

  Betrachten Sie folgendes Beispiel:

  - Festplatte 0 enthält Laufwerk C:\.
  - Volume C:\ enthält das bereitgestellte Volume V:\.
  - Volume V:\ enthält das bereitgestellte Volume W:\.

  CA ARCserve Backup kann die VHD-Datei im Volume V:\ nicht finden.

  Um die Datendateien des Volumes W:\ zu schützen, müssen Sie die Aktualisierung mithilfe des Client Agent für Windows mit CA ARCserve Backup-Agent for Open Files übergeben.

- CA ARCserve Backup erstellt separate Sicherungssitzungen für eingehängte Volumes, die VHDs enthalten.

  Betrachten Sie folgendes Beispiel:

  - Ein Server enthält eine physische Festplatte (C:\), die die VHDs D:\ und E:\ enthält. VHD-Dateien (D.vhd und E.vhd), die sich auf C:\ befinden, werden als Laufwerk D:\ und Laufwerk E:\ bereitgestellt. Laufwerk D:\ wird als C:\MountD bereitgestellt, Laufwerk E:\ als C:\MountE.
  - Wenn Sie C:\MountD sichern und die Option 'Verzeichnisverbindungen und Volume-Bereitstellungspunkte' aktivieren, erstellt CA ARCserve Backup eigene Sicherungssitzungen für die Laufwerke D:\ und C:\MountD.
  - Wenn Sie C:\MountE sichern und die Optionen "Verzeichnisverbindungen und Volume-Bereitstellungspunkte" sowie "Bereitstellungspunkte als Bestandteil des bereitstellenden Volumes sichern" aktivieren, erstellt CA ARCserve Backup eigene Sicherungssitzungen für die Laufwerke E:\ und C:\MountE.

  Hinweis: Die folgenden Optionen sind im Wiederherstellungs-Manager, unter "Globale Optionen", im Dialogfeld "Erweitert" zu finden:

  - Verzeichnisverbindungen und Volume-Bereitstellungspunkte verfolgen
  - Bereitstellungspunkte als Bestandteil des bereitstellenden Volumes sichern

So schützt der Agent freigegebene Clustervolumes

Dieser Abschnitt enthält folgende Themen:

Übersicht über freigegebene Clustervolumes

Mit CA ARCserve Backup können Sie virtuelle Rechner auf CSVs mithilfe des CA ARCserve Backup Agent für virtuelle Rechner schützen.

Ein CSV (Cluster Shared Volume, engl. für: Freigegebenes Clustervolume) ist eine Windows Server 2008 R2-Funktion, mit der Sie mehrere Hyper-V-VMs bündeln können, die über eine Reihe von Cluster-Knoten verteilt sind. Die gebündelten Hyper-V-VMs können auf alle in den CSVs geladenen Dateien gleichzeitig zugreifen.

Obwohl Sie Dateien jeden Typs in CSVs speichern können, empfiehlt Microsoft, dass Sie nur VMs in CSVs erstellen. Als Best Practice ist es ratsam, diese Empfehlung zu beachten und die auf den VMs befindlichen Daten mithilfe des Agent für virtuelle Rechner zu sichern.

CA ARCserve Backup ermöglicht den Schutz von CSVs, die sich auf von Hyper-V konfigurierten Systemen befinden, mithilfe der Microsoft-Technologie Volumenschattenkopie-Dienst. Der Microsoft Volumenschattenkopie-Dienst ist eine Komponente, die in CA ARCserve Backup Agent for Open Files integriert ist. Weitere Informationen finden Sie im *Administrationshandbuch*.

Beschränkungen beim Schutz von freigegebenen Clustervolumes

Beachten Sie folgende Einschränkungen bei der Sicherung von CSVs:

- Knoten, die CSVs freigeben, müssen Zugriff auf die freigegebenen Volumes erhalten. Die freigegebenen Volumes sind im folgenden Verzeichnis zu finden:

  ```
  <Systemlaufwerk>\ClusterStorage
  ```

- Sicherungen von Knoten, die CSVs freigeben, können nicht gleichzeitig durchgeführt werden. Dadurch wird sichergestellt, dass der zu sichernde Knoten während der Sicherung die vollständige Kontrolle über Eingabe- und Ausgabevorgänge des freigegebenen Speichers besitzt. Beispiel: Knoten A und Knoten B geben CSV 1frei. Sie übergeben Jobs, um Knoten A und Knoten B zu sichern. Die Sicherung von Knoten B darf erst nach dem Abschluss der Sicherung von Knoten A beginnen.

- Beim Übergeben von Sicherungen von virtuellen Rechnern, die sich in CSVs in Hyper-V-Systemen befinden, müssen Sie das Windows-Domänenkonto für die Hyper-V-Systeme in der Quellbaumstruktur des Sicherungs-Managers angeben. Zusätzlich muss das Windows-Domänenkonto im Hyper-V-System über die Berechtigungen eines Sicherungsoperators und Cluster-Administrators verfügen. Dadurch wird sichergestellt, dass Sicherungen von virtuellen Rechnern, die sich in CSVs in Hyper-V-Systemen befinden, erfolgreich abgeschlossen werden. Wenn für Hyper-V-Systeme keine gültigen Anmeldeinformationen für die Domäne angegeben werden, schlagen Sicherungsjobs fehl, und es wird folgende Meldung angezeigt:

  ```
  AE0603   VSS-Schattenkopie konnte für VM auf dem Hyper-V-Hostrechner nicht
  erstellt werden.
  ```

Kapitel 5: Wiederherstellen von Daten

Dieses Kapitel enthält folgende Themen:

Wiederherstellen von VMware-VM-Daten

Dieser Abschnitt enthält folgende Themen:

Durchsuchen von VMware-Sitzungen

Sie verwenden zur Wiederherstellung von Daten, die sich in einer VM befinden, denselben Prozess wie bei der Wiederherstellung von einem beliebigen anderen physischen Server.

Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

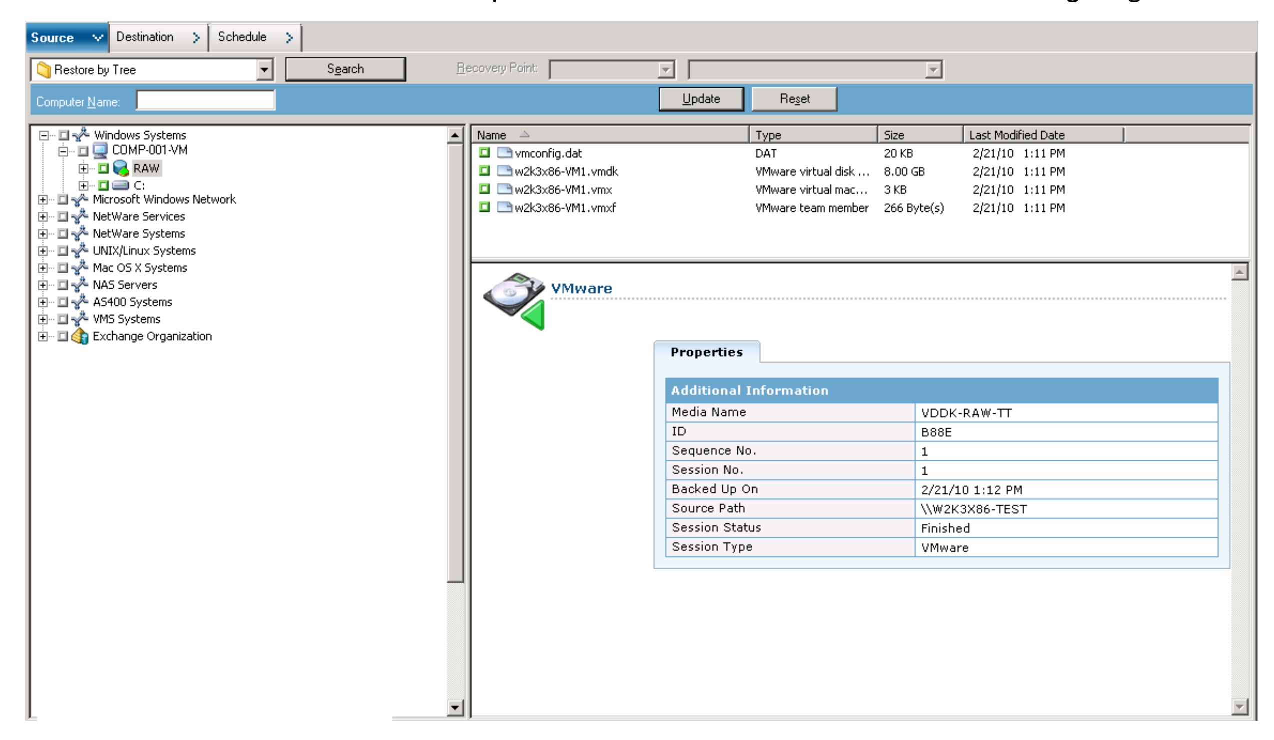
Allerdings weist die Wiederherstellung von Daten von einer VM folgende Einschränkungen auf:

- Sie können Sicherungen auf Dateiebene (Dateimodus) an deren ursprünglichen Speicherort oder einem anderen Speicherort wiederherstellen.

  Hinweis: Um Dateien an ihrem ursprünglichen Speicherort auf einer VM wiederherzustellen, muss der Client Agent für Windows auf der VM installiert sein.

- Sie können Sicherungen auf Raw-Ebene (vollständige VM) nur an einem anderen Speicherort wiederherstellen.

Wenn Sie im Wiederherstellungs-Manager auf der Registerkarte "Quelle" die Option "Wiederherstellung nach Baumstruktur" ausgewählt haben, werden die Raw-Modus (vollständige VM) durchgeführten VM-Sicherungen als VMware-Raw-Image angezeigt. Wenn Sie Sicherungen im Dateimodus durchführen, werden die entsprechenden Volumes des virtuellen Rechners angezeigt.



Im Eigenschaftenbereich der Sitzung im Fenster "Wiederherstellungs-Manager" werden die folgenden Informationen über die VMware-Sicherungsdaten angezeigt:

- **VMware-Proxy:** Gibt den Namen des Sicherungs-Proxy-Systems an, das für die Sicherung dieses VM verwendet wurde.
- **VMware vCenter Server/VMware ESX Host:** Gibt den Namen des VMware ESX Host- oder vCenter Server-Systems an, auf dem der virtuelle Rechner beim Übergeben des Sicherungsjobs ausgeführt wurde.
- **Hostname:** Gibt den Hostnamen des VM an, der am Sicherungsjob beteiligt ist.
- **Sitzungsmethode:** Gibt die Sicherungsmethode an, die zur VM-Sicherung verwendet wurde (z. B. "Raw" und "Datei").

Wiederherstellen von VMs mithilfe von vSphere

Die Methode des Agenten zur Wiederherstellung virtueller Rechner hängt von der Vorgehensweise ab, die beim Sichern der virtuellen Rechner verwendet wurde.

Hinweis: Weitere Informationen zu Sicherungsmethoden finden Sie unter Festlegen von Sicherungsmethoden (siehe Seite 51).

Die folgenden Faktoren sind für VCB-Framework-Sicherungen zu berücksichtigen:

- VMware Converter (Standalone-Version) oder VDDK können zum Wiederherstellen von VCB-Sicherungsdaten verwendet werden.
- Wenn VDDK und VMware Converter (eigenständig) auf dem Sicherungs-Proxy-System installiert werden und Sie virtuelle Rechner auf ESX Server 4.0 oder ESX Server 4.1 wiederherstellen, verwendet der Agent VDDK, um den virtuellen Rechner wiederherzustellen.
- Wenn VDDK und VMware Converter (eigenständig) auf dem Sicherungs-Proxy-System installiert werden und Sie virtuelle Rechner auf ESX Server 3.5 wiederherstellen, verwendet der Agent VMware Converter, um den virtuellen Rechner wiederherzustellen.
- Wenn VDDK auf dem Sicherungs-Proxy-System installiert ist, VMware Converter jedoch nicht, verwendet der Agent VDDK, um die virtuellen Rechner wiederherzustellen.
- Mithilfe von VDDK können Sie Daten virtueller Rechner wiederherstellen, die mithilfe von ESX Server 3.5 oder ESX Server 4.0 gesichert wurden, wenn die Sicherung mithilfe von CA ARCserve Backup r12 SP2, CA ARCserve Backup r12.5 SP1, CA ARCserve Backup r15.0 und CA ARCserve Backup r15 SP1 ausgeführt wurde.

Die folgenden Faktoren sind für VDDK-Sicherungen zu berücksichtigen:

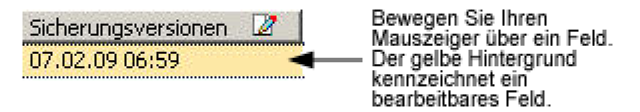
- VDDK-Sicherungsdaten müssen mit VDDK wiederhergestellt werden. VMware Converter kann zum Wiederherstellen von VDDK-Sicherungen nicht verwendet werden.
- ESX Server 3.5 und ESX Server 4.0 können verwendet werden, um VM-Daten wiederherzustellen, die mit ESX Server 3.5 gesichert wurden.
- ESX Server 3.5 kann nicht zum Wiederherstellen von VM-Daten verwendet werden, die mit ESX Server 4.0 gesichert wurden.
- Beim Wiederherstellen von VDDK-Sicherungsdaten mit VDDK ist für den Wiederherstellungsprozess kein freier Speicherplatz auf dem Sicherungs-Proxy-System erforderlich.
- Beim Wiederherstellen von VCB-Sicherungsdaten mit VDDK werden die Daten vom Wiederherstellungsprozess auf dem Sicherungs-Proxy-System wiederhergestellt, die Sicherungsdaten werden von VDDK gelesen, und die Daten werden dann von VDDK auf dem ESX Server-System wiederhergestellt.

Wiederherstellen virtueller VMware-Rechner

Beim Wiederherstellen von VMware-VMs können Sie den gesamten virtuellen Rechner und seine Daten wiederherstellen. Mit diesem Vorgang können Sie Desaster Recovery für eine VM durchführen oder eine VM klonen.

Durchsuchen des Fensters "VM wiederherstellen"

Mithilfe des Fensters "VM wiederherstellen" können Sie verschiedene Felder durchsuchen, auswählen und ändern. Wenn Sie den Mauszeiger über ein bearbeitbares Feld führen, wird der Hintergrund des Feldes gelb angezeigt.



Um ein bearbeitbares Feld zu ändern, wählen Sie das Zielfeld, und klicken Sie dann auf die Auslassungspunkte, um das Feld zu durchsuchen.



Besondere Aspekte

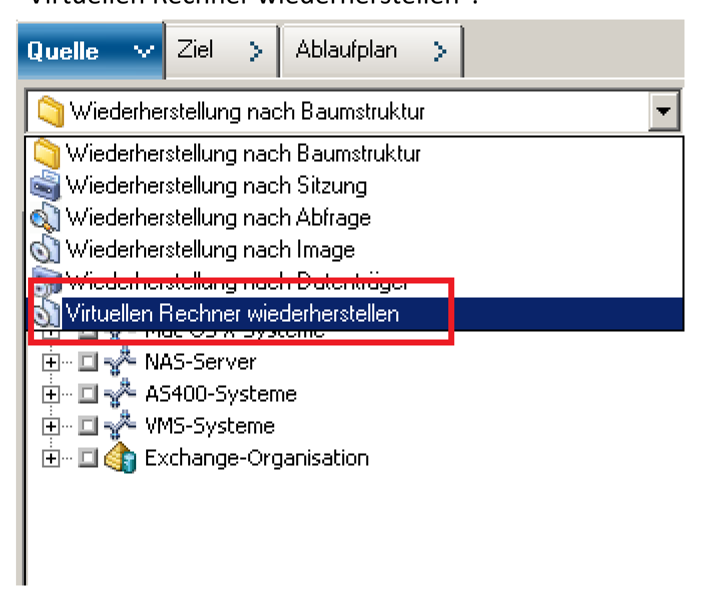
Beachten Sie Folgendes:

- CA ARCserve Backup stellt die Sicherungsdaten des virtuellen Rechners auf dem Sicherungs-Proxy-System an einem temporären Ladeort wieder her und stellt die Daten anschließend im VMware ESX Host-System wieder her.
- Auf dem Sicherungs-Proxy-System muss VMware Converter in der Version 3.0.2 oder später installiert sein. CA ARCserve Backup verwendet die Tools von VMware Converter, um VCB-Images virtueller Rechner wiederherzustellen. Es ist nicht erforderlich, dass VMware Converter Daten virtueller Rechner wiederherstellt, die mithilfe von VDDK gesichert wurden.

  Hinweis: Informationen zum VMware Converter finden Sie unter www.vmware.com/de/products/converter.

So stellen Sie virtuelle VMware-Rechner wieder her:

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Drop-down-Liste die Option "Virtuellen Rechner wiederherstellen".

   Das Fenster "Virtuellen Rechner wiederherstellen" wird geöffnet.

2. Führen Sie eine der folgenden Aktionen aus, um nach einer VMware-VM zu suchen, und fahren Sie dann mit dem nächsten Schritt fort.

   - Um nach einer bestimmten VM zu suchen, geben Sie im Feld für den Namen des virtuellen Rechners den Namen der VM an, und klicken Sie auf "Abfragen".

     Der gesuchte VM-Name wird in der Liste der VMs angezeigt.

   - Um nach allen VMs zu suchen, wählen Sie im Feld für den Namen des virtuellen Rechners die Option << ALLE >> aus, und klicken Sie auf "Abfragen".

     Alle VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

   - Um nach einem unvollständigen VM-Namen zu suchen, ersetzen Sie die unbekannten Zeichen durch einen Stern (*), und klicken Sie auf "Abfragen".

     Die VMs, die den Suchkriterien entsprechen, werden in der Liste der VMs angezeigt.

     Beispiel: Wenn Sie den Wert 100-* eingeben, werden die Namen aller VMs zurückgegeben, die mit 100- beginnen, z. B. 100-1, 100-01, and 100-001.

   - Klicken Sie im Feld "Nach virtuellem Rechner suchen" auf "VMware".

     Alle VMware-VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

3. Füllen Sie in der VM-Liste folgende Felder aus.

   - **VM-Name (DNS-Name)** - Aktivieren Sie das Kontrollkästchen neben "VM-Name", um die wiederherzustellenden VMs anzugeben.

     Hinweis: Wenn Sie mehr als eine VM angeben, verarbeitet CA ARCserve Backup die Wiederherstellungsvorgänge sequenziell.

   - **Sicherungsversionen** - Mit dieser Option können Sie eine Sicherungsversion angeben.

     Akzeptieren Sie die angezeigte Sicherungsversion, oder klicken Sie in das Feld "Sicherungsversionen" und dann auf die Auslassungspunkte, um nach mehreren Versionen der Sicherungsdaten zu suchen.

   - **Proxy-Rechner:** Hier können Sie das Sicherungs-Proxy-System und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

     Akzeptieren Sie den angezeigten Proxy-Rechner, oder klicken Sie in das Feld "Proxy-Rechner" und dann auf die Auslassungspunkte, um nach einem anderen Sicherungs-Proxy-System zu suchen und dieses auszuwählen.

- **Pfad:** Hier können Sie den Pfad zum Laden des VM-Images angeben.

  Akzeptieren Sie den angezeigten Pfad, oder klicken Sie in das Feld "Pfad", um einen alternativen Pfad für das temporäre VM-Ladeverzeichnis anzugeben.

- **VMware ESX-Hostname:** Hier können Sie den ESX Server und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

  Akzeptieren Sie den angezeigten VMware ESX-Hostnamen, oder klicken Sie in das Feld "VMware ESX-Hostname" und dann auf die Auslassungspunkte, um ein alternatives VMware ESX-Hostsystem zu suchen und festzulegen.

- **Datenspeicher:** Ermöglicht das Festlegen des Datenspeichers, das mit dem VMware ESX-Hostsystem verbunden ist.

  Akzeptieren Sie den angezeigten, mit dem VMware ESX-Hostsystem verbundenen Datenspeichernamen, oder klicken Sie in das Feld "Datenspeicher", um den Datenspeicher des VMware ESX-Hostsystems festzulegen.

  Hinweis: Beim Datenspeicher ist die Groß- und Kleinschreibung zu beachten.

4. Klicken Sie in der Symbolleiste auf "Optionen".

   Das Dialogfeld "Globale Optionen" wird geöffnet.

5. Klicken Sie auf die Registerkarte "Vorgang", und legen Sie folgende Optionen fest:

   Hinweis: Die folgenden Optionen werden nicht auf der Registerkarte "Vorgang" angezeigt, es sei denn, die Methode "Virtuellen Rechner wiederherstellen" wurde festgelegt.

   - **VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten -** Schaltet die VM nach Abschluss des Wiederherstellung ein.

     Standardwert: Aktiviert.

     Beispiel: Legen Sie diese Option fest, wenn Sie den virtuellen Rechner unmittelbar nach Abschluss der Wiederherstellung verwenden müssen.

   - **VMware-VM überschreiben, falls vorhanden:** Hiermit können Sie eine ggf. vorhandene VM überschreiben.

     Standardwert: Aktiviert.

     Wenn Sie eine VMware-VM wiederherstellen, ermittelt CA ARCserve Backup die virtuellen Rechner, die sich auf dem Hostsystem befinden. Falls der virtuelle Rechner auf dem Hostsystem vorhanden ist, können Sie ihn mit dieser Option unter Verwendung der bestehenden UUID und Hostnamens des virtuellen Rechners überschreiben.

     Hinweis: Informationen zur Fehlerbehebung finden Sie unter Der Agent löscht vorhandene VMs nicht, nachdem ein VM-Wiederherstellungsjob abgeschlossen ist (siehe Seite 147).

6. Klicken Sie auf "OK".

   Die Optionen werden übernommen.

7. Klicken Sie auf die Sendeschaltfläche, um den Wiederherstellungsjob zu senden.

   Das Dialogfeld "Job übergeben" wird angezeigt.

8. Wählen Sie im Dialogfeld "Job übergeben" die Option "Jetzt ausführen" aus, um den Job sofort zu starten, oder wählen Sie "Ausführen am" aus, und geben Sie ein Datum und eine Uhrzeit für den Job an.

   Geben Sie eine Beschreibung für den Job ein, und klicken Sie auf "OK".

   Der Job wird übergeben.

   Hinweis: Weitere Informationen zum Übergeben von Jobs finden Sie im *Administrationshandbuch*.

Wiederherstellen von Hyper-V-VM-Daten

Dieser Abschnitt enthält folgende Themen:

Durchsuchen von Hyper-V-Sitzungen

Sie verwenden zur Wiederherstellung von Daten, die sich in einer VM befinden, denselben Prozess wie bei der Wiederherstellung von einem beliebigen anderen physischen Server.

Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

Allerdings weist die Wiederherstellung von Daten von einer VM folgende Einschränkungen auf:

- Sie können Sicherungen auf Dateiebene (Dateimodus) an deren ursprünglichen Speicherort oder einem anderen Speicherort wiederherstellen.

  Hinweis: Um Dateien an ihrem ursprünglichen Speicherort auf einer VM wiederherzustellen, muss der Client Agent für Windows auf der VM installiert sein.

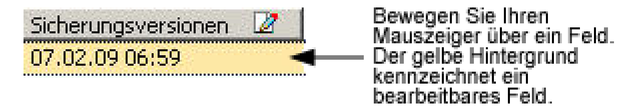
- Sie können Sicherungen auf Raw-Ebene (vollständige VM) nur an einem anderen Speicherort wiederherstellen.

Wiederherstellen virtueller Hyper-V-Rechner

Beim Wiederherstellen von Hyper-V-VMs können Sie den gesamten virtuellen Rechner sowie dessen Daten wiederherstellen. Mit diesem Vorgang können Sie Desaster Recovery für eine VM durchführen oder eine VM klonen.

Durchsuchen des Fensters "VM wiederherstellen"

Mithilfe des Fensters "VM wiederherstellen" können Sie verschiedene Felder durchsuchen, auswählen und ändern. Wenn Sie den Mauszeiger über ein bearbeitbares Feld führen, wird der Hintergrund des Feldes gelb angezeigt.



Um ein bearbeitbares Feld zu ändern, wählen Sie das Zielfeld, und klicken Sie dann auf die Auslassungspunkte, um das Feld zu durchsuchen.



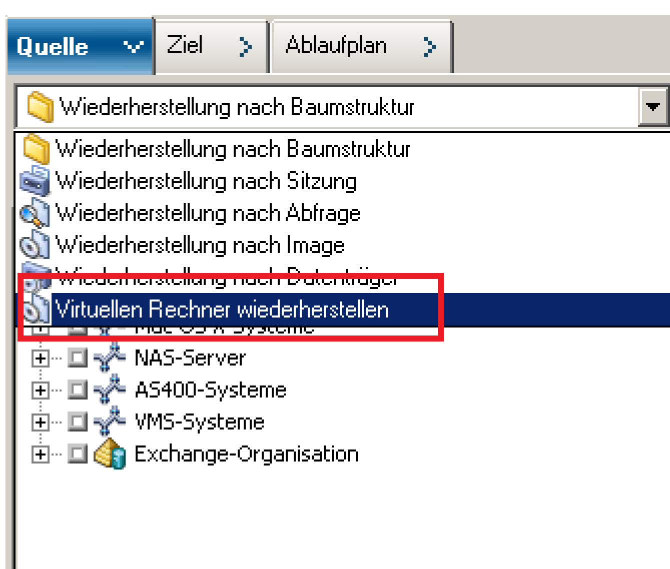
Besondere Aspekte

Beachten Sie Folgendes:

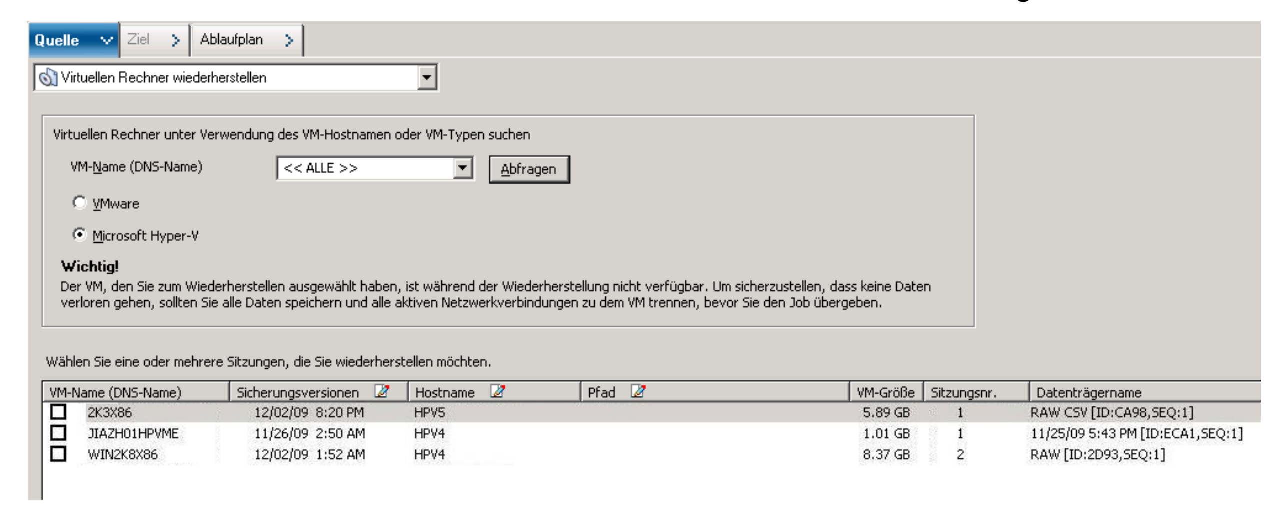
- Die Ziel-VM sollte ausgeschaltet werden und vom System gelöscht oder umbenannt werden. Wenn die VM nicht heruntergefahren und gelöscht oder umbenannt wird, werden die Daten auf der Ziel-VM während des Wiederherstellungsvorgangs überschrieben.

So stellen Sie virtuelle Hyper-V-Rechner wieder her:

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Drop-down-Liste die Option "Virtuellen Rechner wiederherstellen".



Das Fenster "Virtuellen Rechner wiederherstellen" wird geöffnet.



2. Führen Sie eine der folgenden Aktionen aus, um nach einem Hyper-V-VM zu suchen, und fahren Sie dann mit dem nächsten Schritt fort.

   - Um nach einer bestimmten VM zu suchen, geben Sie im Feld für den Namen des virtuellen Rechners den Namen der VM an, und klicken Sie auf "Abfragen".

     Der gesuchte VM-Name wird in der Liste der VMs angezeigt.

   - Um nach allen VMs zu suchen, wählen Sie im Feld für den Namen des virtuellen Rechners die Option << ALLE >> aus, und klicken Sie auf "Abfragen".

     Alle VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

   - Um nach einem unvollständigen VM-Namen zu suchen, ersetzen Sie die unbekannten Zeichen durch einen Stern (*), und klicken Sie auf "Abfragen".

     Die VMs, die den Suchkriterien entsprechen, werden in der Liste der VMs angezeigt.

     Beispiel: Wenn Sie den Wert 100-* eingeben, werden die Namen aller VMs zurückgegeben, die mit 100- beginnen, z. B. 100-1, 100-01, and 100-001.

   - Klicken Sie im Feld "Nach virtuellem Rechner suchen" auf "Hyper-V".

     Alle Hyper-V-VMs Ihrer Umgebung werden in der VM-Liste angezeigt.

3. Füllen Sie in der VM-Liste folgende Felder aus.

   - **VM-Name (DNS-Name)** - Aktivieren Sie das Kontrollkästchen neben "VM-Name", um die wiederherzustellenden VMs anzugeben.

     Hinweis: Wenn Sie mehr als eine VM angeben, verarbeitet CA ARCserve Backup die Wiederherstellungsvorgänge sequenziell.

   - **Sicherungsversionen** - Mit dieser Option können Sie eine Sicherungsversion angeben.

     Akzeptieren Sie die angezeigte Sicherungsversion, oder klicken Sie in das Feld "Sicherungsversionen" und dann auf die Auslassungspunkte, um nach mehreren Versionen der Sicherungsdaten zu suchen.

   - **Hostname:** Hier können Sie das Hyper-V-Hostsystem und die Sicherheitsinformationen angeben, die für die Wiederherstellung des VM-Images erforderlich sind.

     Wenn Sie das Hyper-V-System auf einem anderen Hyper-V-Host wiederherstellen wollen, müssen Sie das Verzeichnis angeben, auf dem Sie das VM-Image wiederherstellen wollen.

   - **Pfad:** Ermöglicht die Angabe des Pfads, auf dem Sie das VM-Image wiederherstellen wollen.

     Hinweis: Wenn das Feld "Pfad" leer ist, stellt CA ARCserve Backup das VM-Image an seinem ursprünglichen Speicherort wieder her.

4. Klicken Sie in der Symbolleiste auf "Optionen".

   Das Dialogfeld "Globale Optionen" wird geöffnet.

5. Klicken Sie auf die Registerkarte "Vorgang", und legen Sie die folgende Option fest:

   Hinweis: Die folgende Option wird auf der Registerkarte "Vorgang" nicht angezeigt, es sei denn, die Methode "Virtuellen Rechner wiederherstellen" wurde festgelegt.

   - **VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten -** Schaltet die VM nach Abschluss des Wiederherstellung ein.

     Standardwert: Aktiviert.

     Beispiel: Legen Sie diese Option fest, wenn Sie den virtuellen Rechner unmittelbar nach Abschluss der Wiederherstellung verwenden müssen.

6. Klicken Sie auf "OK".

   Die Optionen werden übernommen.

7. Klicken Sie auf die Sendeschaltfläche, um den Wiederherstellungsjob zu senden.

   Das Dialogfeld "Job übergeben" wird angezeigt.

8. Wählen Sie im Dialogfeld "Job übergeben" die Option "Jetzt ausführen" aus, um den Job sofort zu starten, oder wählen Sie "Ausführen am" aus, und geben Sie ein Datum und eine Uhrzeit für den Job an.

   Geben Sie eine Beschreibung für den Job ein, und klicken Sie auf "OK".

   Der Job wird übergeben.

   Hinweis: Weitere Informationen zum Übergeben von Jobs finden Sie im *Administrationshandbuch*.

Wiederherstellen von virtuellen Hyper-V-VMs auf alternativen Hosts

CA ARCserve Backup ermöglicht das Wiederherstellen von Hyper-V-Sicherungsdaten an einem alternativen Speicherort und den Schutz von VMs, die sich auf ungenannten Volumen befinden.

Hinweis: Ein unbenanntes Volume ist ein Volume, dem kein Laufwerkbuchstabe zugewiesen ist.

Mit diesen Funktionen können Sie Folgendes tun:

- Virtuelle Rechner (VMs) an demselben oder einem anderen Windows Server 2008 Hyper-V-System wiederherstellen.
- Verzeichnisse (mit oder ohne Laufwerkbuchstaben) während des Wiederherstellungsprozesses auf den Ziel-VMs erstellen, wenn zuvor keine Verzeichnisse vorhanden sind.

Der VM-Wiederherstelllungsbildschirm des Wiederherstellungs-Managers enthält Steuerelemente, die folgende Aufgaben ermöglichen:

- Wiederherstellen von Hyper-V-VMs an einem alternativen Speicherort, wobei es sich beim Hyper-V-Server um ein Windows Server 2008 R2 Hyper-V-System handelt.
- Festlegen von Pfaden für den alternativen Speicherort auf dem Zielsystem Windows Server 2008 R2 Hyper-V.

Beachten Sie Folgendes:

- Wenn Sie einen alternativen Speicherort angeben, übernimmt CA ARCserve Backup den gesamten Pfad des Sicherungssatzes, mit Ausnahme des Stammlaufwerks oder Volume-Namens, und fügt diesen dem angegebenen Pfad hinzu.

Daten auf Dateiebenengranularität wiederherstellen

Dieses Thema beschreibt, wie Daten wiederhergestellt werden, die in folgenden Sicherungsmodi gesichert wurden:

- Dateimodus
- Raw-Modus mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren"
- Gemischter Modus mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren"

  Hinweis: Weitere Informationen finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

Anhand dieser Schritte können Sie Wiederherstellungsvorgänge auf lokalen, festplattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs durchführen. Sie stellen Daten, die auf einer VM gesichert wurden, auf Dateiebene wieder her, wenn eine Datei beschädigt oder versehentlich gelöscht wurde, um ein System nach einem Ausfall wiederherzustellen oder um ein System zu klonen. Sie verwenden zur Wiederherstellung von Sicherungen auf Dateiebene denselben Prozess wie bei der Wiederherstellung von einer beliebigen Windows-basierten Client Agent-Datei.

Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

Beim Wiederherstellen von Sicherungsdaten auf Dateiebene ist Folgendes zu beachten:

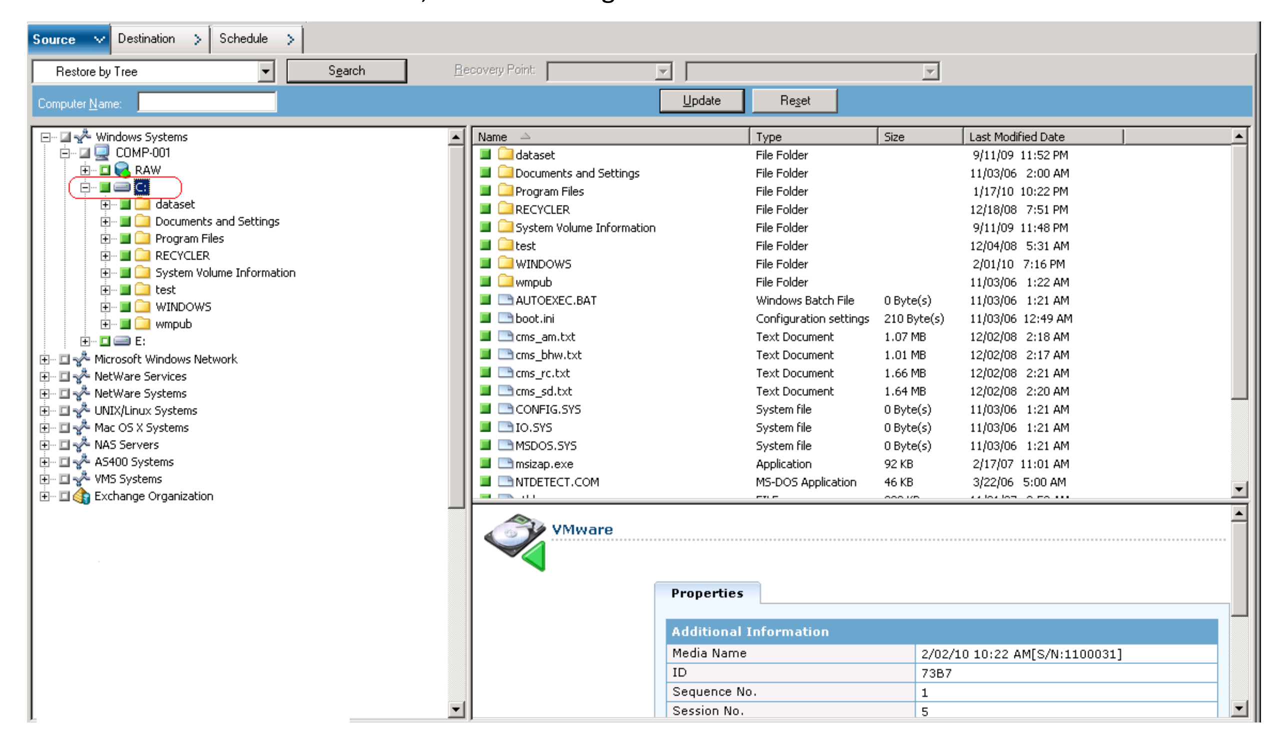
- Sie können Daten nur dann durchsuchen und auf Verzeichnis- und Dateiebenengranularität wiederherstellen, wenn die Daten im Dateimodus, im Raw-Modus (vollständige VM) mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" oder im gemischten Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" gesichert wurden.

  Hinweis: Weitere Informationen finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

- Die aktuelle Version des Client Agent für Windows muss auf dem Zielsystem installiert sein, damit Daten wiederhergestellt werden können, die mithilfe des Agenten für virtuelle Rechner gesichert wurden.
- Wenn Sie Daten auf Dateiebenengranularität wiederherstellen und die Option "'Dateien am ursprünglichen Speicherort wiederherstellen" aktivieren, werden Windows-Systemdateien von CA ARCserve Backup absichtlich ausgelassen. Windows-Systemdateien sind normalerweise in den folgenden Verzeichnissen gespeichert:
  - C:\WINDOWS\SYSTEM
  - C:\WINDOWS\SYSTEM32

So stellen Sie Daten auf Dateiebenengranularität wieder her

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Drop-down-Liste die Option "Wiederherstellung nach Baumstruktur".
2. Erweitern Sie das Objekt "Windows-Systeme", und navigieren Sie zu den Daten, die wiederhergestellt werden sollen.



3. Klicken Sie auf die Registerkarte "Ziel". Aktivieren Sie das Kontrollkästchen "Dateien am ursprünglichen Speicherort wiederherstellen", um die Dateien an dem ursprünglichen Speicherort wiederherzustellen.

   Wenn Sie Dateien am ursprünglichen Speicherort wiederherstellen möchten, muss der Client Agent für Windows auf der VM installiert sein. Wenn der Client Agent für Windows auf der VM nicht installiert ist, können Sie Daten an einem beliebigen Speicherort wiederherstellen und anschließend mithilfe einer Netzwerk-Dateisystemfreigabe manuell auf den VM kopieren.

   Hinweis: Wenn Sie Daten auf Dateiebenengranularität wiederherstellen und die Option "'Dateien am ursprünglichen Speicherort wiederherstellen" aktivieren, werden Windows-Systemdateien von CA ARCserve Backup ausgelassen.

   Wichtig! Um VMware-basierte Sicherungssitzungen an einem alternativen Speicherort wiederherzustellen, muss der Client Agent für Windows auf dem alternativen System laufen, und das alternative System muss unter dem Objekt "Windows-Systeme" angezeigt werden. Wenn Sie versuchen, Daten auf einem System wiederherzustellen, das nicht unter dem Objekt "Windows-Systeme" angezeigt wird, schlägt der Wiederherstellungsjob fehl. Um Daten an einem alternativen Speicherort auf einem lokalen System wiederherzustellen, auf dem ein Windows-X86-Betriebssystem ausgeführt wird, fügen Sie im Wiederherstellungs-Manager auf der Registerkarte "Ziel" das System mit einem fiktiven Hostnamen und der echten IP-Adresse unter dem Objekt "Windows-Systeme" hinzu. Dann können Sie das Ziel als das lokale System angeben und den Wiederherstellungsjob übergeben.

   Falls die Sicherungsdaten von einer Sicherung im Raw-Modus (vollständige VM) erstellt wurden, unterstützt CA ARCserve Backup die Option "Dateien am ursprünglichen Speicherort wiederherstellen" nicht.

4. Klicken Sie auf die Registerkarte "Ablaufplan", und wählen Sie aus der Drop-down-Liste eine "Wiederholungsmethode" aus.

5. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Übergeben", um den Wiederherstellungsjob zu übergeben.

   Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet. Um den Job zu übergeben, müssen Sie für das System, auf dem die Daten wiederhergestellt werden, Ihre Anmeldeinformationen angeben.

6. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

   CA ARCserve Backup wendet Ihre Sicherheitsinformationen an, und das Dialogfeld "Job übergeben" wird geöffnet.

7. Nehmen Sie die Eingaben in den Feldern im Dialogfeld "Job übergeben" vor, und klicken Sie auf "OK".

   Der Job wird übergeben.

   Hinweis: Klicken Sie im Dialogfeld "Job übergeben" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch*.

Wiederherstellen von Sicherungsdaten auf Raw-Ebene (vollständige VM)

Führen Sie mit den folgenden Schritten Wiederherstellungsvorgänge auf lokalen, festplattenbasierten virtuellen Rechnern (VMs) und SAN-basierten VMs durch. Eine Wiederherstellung von Raw-Daten (vollständige VM-Sicherung) wird im Rahmen der Disaster Recovery erforderlich oder wenn ein System geklont werden soll. Sie verwenden zur Wiederherstellung von Sicherungen auf Dateiebene denselben Prozess wie bei der Wiederherstellung von einer beliebigen Windows-basierten Client Agent-Datei.

Hinweis: Weitere Informationen zum Wiederherstellen von Daten finden Sie im *Administrationshandbuch*.

Beim Wiederherstellen von Sicherungsdaten auf Raw-Ebene ist Folgendes zu beachten:

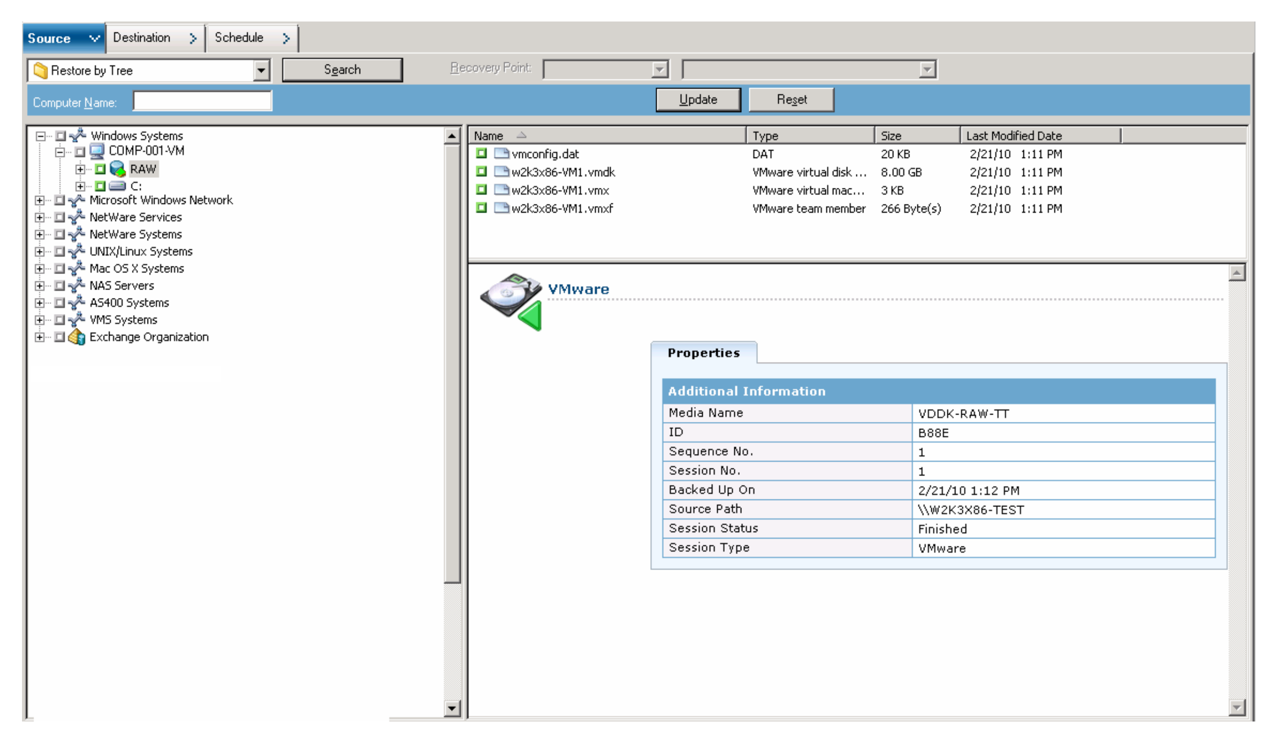
- Die aktuelle Version des Client Agent für Windows muss auf dem Zielsystem installiert sein, damit Daten wiederhergestellt werden können, die mithilfe des Agenten für virtuelle Rechner gesichert wurden.
- Daten, die im Raw-Modus (vollständige VM) oder gemischten Modus bei deaktivierter Option "Wiederherstellung im Dateimodus erlauben" gesichert wurden, können nicht auf Verzeichnis- oder Dateiebene durchsucht und wiederhergestellt werden.

So stellen Sie Daten auf Raw-Ebene (vollständige VM) wieder her

1. Öffnen Sie den Wiederherstellungs-Manager, klicken Sie auf die Registerkarte "Quelle", und wählen Sie aus der Drop-down-Liste die Option "Wiederherstellung nach Baumstruktur".

   Erweitern Sie das Objekt "Windows-Systeme", und navigieren Sie zu dem VMware-System oder Hyper-V-System, das wiederhergestellt werden soll.

   Erweitern Sie das gewünschte System, und wählen Sie die Daten aus, die Sie wiederherstellen möchten.



2. Klicken Sie auf die Registerkarte "Ziel".

   Geben Sie den Speicherort für die Wiederherstellung der Daten an.

3. Klicken Sie auf die Registerkarte "Ablaufplan", und wählen Sie aus der Drop-down-Liste eine "Wiederholungsmethode" aus.

4. Klicken Sie auf der Symbolleiste auf die Schaltfläche "Übergeben", um den Wiederherstellungsjob zu übergeben.

   Das Dialogfeld "Sicherheits- und Agent-Informationen" wird geöffnet. Um den Job zu übergeben, müssen Sie für das System, auf dem die Daten wiederhergestellt werden, Ihre Anmeldeinformationen angeben.

5. Geben Sie Ihre Anmeldeinformationen in den Feldern "Benutzername" und "Kennwort" ein, und klicken Sie auf "OK".

   CA ARCserve Backup wendet Ihre Sicherheitsinformationen an, und das Dialogfeld "Job übergeben" wird geöffnet.

6. Nehmen Sie die Eingaben in den Feldern im Dialogfeld "Job übergeben" vor, und klicken Sie auf "OK".

   Der Job wird übergeben.

   Hinweis: Klicken Sie im Dialogfeld "Job übergeben" auf die Schaltfläche "Hilfe", um weitere Informationen zum Übergeben von Jobs anzuzeigen. Weitere Informationen über die Anzeige des Jobstatus und andere jobbezogene Aufgaben finden Sie im *Administrationshandbuch*.

Anhang A: Fehlerbehebung

Dieses Kapitel enthält folgende Themen:

Sicherungs- und Wiederherstellungsvorgänge

In den folgenden Themen wird beschrieben, wie Sie Fehler bei Sicherungs- und Wiederherstellungsvorgängen auf Systemen beheben, auf denen VMware vSphere ausgeführt wird.

Die automatische Aufnahme des VM-Prozesses wird nicht gemäß Ablaufplan gestartet

Betrifft alle Windows-Betriebssysteme, die von CA ARCserve Backup unterstützt werden.

Symptom:

Die automatische Aufnahme des VM-Prozesses wird nicht gemäß Ablaufplan gestartet Die Häufigkeit der automatischen Aufnahme wurde vor kurzem geändert.

Lösung:

Nach dem Ändern der Häufigkeit der automatischen Aufnahme wird der Prozess am nächsten Kalendertag gestartet.

Beispiel: Ändern der Häufigkeit der automatischen Aufnahme des VM-Prozesses

Am 5. April ändern Sie um 11:00 Uhr die Häufigkeit der automatischen Aufnahme des VM-Prozesses in eine Stunde. Sie erwarten, dass der Prozess am 5. April um 12:00 Uhr gestartet wird, was jedoch nicht der Fall ist. Die automatische Aufnahme des VM-Prozesses beginnt am 6. April um 12:00 Uhr und wird jede Stunde ausgeführt.

Auf dem Sicherungs-Proxy-System werden keine Protokolldateien zum Agenten für virtuelle Rechner angezeigt.

Gilt für alle Windows-Betriebssysteme, die als Sicherungs-Proxy-Systeme eingesetzt werden.

Symptom:

Die Protokolldateien "MntJrnl.log" und "vcbmounter_outputxxxx.log" werden im Protokollverzeichnis des Client Agent auf dem Sicherungs-Proxy-System nicht angezeigt.

Lösung:

Dies tritt beim Sichern von VM-Daten mithilfe von VDDK auf. VDDK verwendet zum Bearbeiten von VCB-Sicherungen nicht die VMware-Komponente "vcbmounter". Daher werden bei der Sicherung nicht die Protokolldateien "MntJrnl.log" und "vcbmounter_outputxxxx.log" zum Ladevorgang generiert.

Der vcbmounter-Prozess wird nach dem Abbrechen von Sicherungsjobs nicht beendet

Gilt für alle Windows-Betriebssysteme, die als Sicherungs-Proxy-Systeme eingesetzt werden.

Symptom:

Der vcbmounter-Prozess wird auf dem Sicherungs-Proxy-System nicht beendet, nachdem ein VCB-Framework-Sicherungsjob abgebrochen wird.

Lösung:

Obwohl VMware VCB Framework-Sicherungsjobs abgebrochen werden können, werden die Lade- und Exportvorgänge nicht beendet, die mit VCB Framework-Sicherungen verknüpft sind. VCB Framework stellt keine Option bereit, mit der VCBMounter-Lade- und Exportvorgänge abgebrochen werden können.

Der Agent löscht vorhandene VMs nicht, nachdem ein VM-Wiederherstellungsjob abgeschlossen ist

Zulässig auf allen unterstützten Windows-Betriebssystemen.

Symptom:

Im folgenden Szenario wird das auf dem ESX Server-System vorhandene VM von CA ARCserve Backup ggf. nicht gelöscht:

- Sie übergeben einen VM-Wiederherstellungsjob.
- Sie haben die Option zum Überschreiben der globalen VM-Wiederherstellung aktiviert.
- CA ARCserve Backup stellt den VM auf dem Sicherungs-Proxy-System erfolgreich wieder her (ESX Server-System).

Lösung:

Hierbei handelt es sich um ein erwartetes Verhalten.

Der Agent verbindet die UUID und den Hostnamen eines VM, um einen einmaligen Bezeichner für den VM zu erstellen. CA ARCserve Backup verwendet den Bezeichner, um Sicherungs- und Wiederherstellungsvorgänge für den entsprechenden VM zu unterscheiden. VMware vSphere verwendet die UUID jedoch nicht mehr als einen Mechanismus, um VMs zu identifizieren. Wenn Sie einen Job übergeben, um den VM wiederzuherstellen, und die Option zum Überschreiben des VM angeben, löscht CA ARCserve Backup den Original-VM nicht, wenn es keinen VM mit der gleichen UUID und den gleichen Hostnamen des Original-VM erkennen kann. Daher erstellt CA ARCserve Backup einen neuen virtuellen Rechner, anstatt den vorhandenen VM zu überschreiben. Dadurch wird sichergestellt, dass CA ARCserve Backup einen VM nicht versehentlich löscht. CA ARCserve Backup zeigt dieses Verhalten außerdem in den folgenden Szenarien:

- Die UUID oder der Hostname des VM wurde verändert.
- Der VM wurde ausgeschaltet oder heruntergefahren (der Agent kann den Hostnamen des VM nicht abrufen).

Sicherungsjobs schlagen anscheinend fehl.

Gilt für Hyper-V- und VMware-Systeme.

Symptom:

Sie übermitteln eine Sicherung von VMware- oder Hyper-V-VMs. Folgende Optionen wurden für die Sicherung festgelegt:

- Raw-Modus oder gemischter Modus
- Wiederherstellung auf Dateiebene aktivieren

Der Job wird mit dem Status "Unvollständig" beendet, und im Aktivitätsprotokoll wird die Fehlermeldung AW0550 angezeigt.

Lösung:

Das oben beschriebene Verhalten tritt auf, da der Name des CA ARCserve Backup-Servers, der die VM schützt, nicht angegeben wurde oder der angegebene Name nicht korrekt ist.

Stellen Sie zur Behebung dieses Fehlers sicher, dass der Name des CA ARCserve Backup-Servers, der die VM schützt, korrekt angegeben ist.

Weitere Informationen finden Sie unter Angeben des CA ARCserve Backup-Servernamens (siehe Seite 69).

Die Datengröße der Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz

Gültig auf Windows-Plattformen.

Symptom:

Die Datengröße der Sicherungssitzungen übersteigt den auf virtuellen Rechnern belegten Speicherplatz.

Lösung:

Dies ist das normale Verhalten, wenn Sie einen Sicherungsjob im Raw-Modus mit aktivierter Option "Wiederherstellung im Dateimodus erlauben" übergeben. Betrachten Sie folgendes Beispiel:

Daten	Größe der Sicherungssitzung mit "Wiederherstellung im Dateimodus erlauben"	Größe der Sicherungssitzung ohne "Wiederherstellung im Dateimodus erlauben"
Virtueller Datenträger: 20 GB **Belegter Speicher:** 4 GB **Freier Speicherplatz:** 16 GB	20 GB	4 GB

Bei *aktivierter* Option "Wiederherstellung im Dateimodus erlauben" sichert CA ARCserve Backup den belegten und den freien Speicherplatz auf dem virtuellen Rechner. Daher entspricht die Größe der Sicherungssitzung der Größe des virtuellen Rechners.

Bei *deaktivierter* Option "Wiederherstellung im Dateimodus erlauben" sichert CA ARCserve Backup nur den belegten Speicherplatz auf dem virtuellen Rechner. Daher ist die Sicherungssitzung etwas größer als der Umfang des belegten Speicherplatzes auf dem virtuellen Rechner. (CA ARCserve Backup reserviert zusätzlichen Platz für Metadaten.)

Fehler bei der Wiederherstellung von virtuellen Rechnern auf virtuellen VMware-Rechnern

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie Jobs zur Wiederherstellung virtueller Rechner auf VMware-basierten virtuellen Rechnern übergeben, tritt der Fehler AE0564 auf.

Lösungen:

Es gibt verschiedene Gründe für Fehler bei der Wiederherstellung virtueller Rechner auf virtuellen VMware-Rechnern. In der folgenden Liste finden Sie mögliche Fehlerursachen sowie die erforderlichen Maßnahmen.

- **Symptom 1:** Die für das VMware ESX-Hostsystem angegebenen Anmeldeinformationen sind falsch.

  Lösung 1: Stellen Sie sicher, dass die für das VMware ESX-Hostsystem angegebenen Anmeldeinformationen richtig sind.

- **Symptom 2:** Der Zieldatenspeicher verfügt nicht über ausreichend freien Speicherplatz.

  Lösung 2: Stellen Sie sicher, dass im Zieldatenspeicher auf dem VMware ESX-Hostsystem ausreichend freier Speicherplatz verfügbar ist. Sie können den Zieldatenspeicher ggf. auch auf ein anderes VMware ESX-Hostsystem verschieben.

- **Symptom 3:** Das VMware ESX-Hostsystem wurde heruntergefahren oder ist nicht erreichbar.

  Lösung 3: Stellen Sie sicher, dass das VMware ESX-Hostsystem mit dem Sicherungs-Proxy-System kommunizieren kann.

- **Symptom 4:** VMware unterstützt das auf dem virtuellen Rechner ausgeführte Gastbetriebssystem nicht.

  Lösung 4: Stellen Sie sicher, dass der VMware Converter das auf dem virtuellen Rechner ausgeführte Gastbetriebssystem unterstützt. Weitere Informationen finden Sie auf der VMware-Support-Website.

  Hinweis: Es ist nicht erforderlich, dass VMware Converter Daten virtueller Rechner wiederherstellt, die mithilfe von VDDK gesichert wurden.

- **Symptom 5:** Sie haben versucht, ein Gastbetriebssystem mit einer x64-Architektur auf einem VMware ESX-Hostsystem mit x86-Architektur wiederherzustellen.

  Lösung 5: Stellen Sie sicher, dass das VMware ESX-Hostsystem über eine x64-Architektur verfügt.

  Hinweis: Zum Wiederherstellen des VM können Sie die VMDK-Dateien verwenden. Den Pfad zu den VMDK-Dateien finden Sie in der Datei "CA_VCBpopulateDB.log", die sich im Sicherungs-Proxysystem befindet. Die Datei "CA_VCBpopulateDB.log" befindet sich in folgendem Verzeichnis:

  ```
  <<Installationsverzeichnis des Client Agent>>\Log
  ```

- **Symptom 6:** VDDK ist auf dem Sicherungs-Proxy-System nicht installiert, und VMware Converter Enterprise ist auf dem Sicherungs-Proxy-System installiert.

  Der Agent für virtuelle Rechner unterstützt die Verwendung von Unternehmensversionen von VMware Converter nicht. Damit die Wiederherstellung von VMs-Jobs erfolgreich abgeschlossen wird, müssen auf dem Sicherungs-Proxy-System Standalone-Versionen von VMware Converter installiert sein.

  Lösung 6: Deinstallieren Sie VMware Converter Enterprise vom Sicherungs-Proxy-System. Installieren Sie eine Standalone-Version von VMware Converter auf dem Sicherungs-Proxy-System.

Sicherungsdaten auf Dateiebene können nicht auf einem CA ARCserve Backup-Server wiederhergestellt werden

Gültig auf Windows-Plattformen.

Symptom:

In CA ARCserve Backup gibt es keinen Mechanismus, mit dem Sicherungsdaten auf Dateiebene auf einem CA ARCserve Backup-Server wiederhergestellt werden können.

Lösung:

Damit Sicherungsdaten auf Dateiebene an einem anderen Standort wiederhergestellt werden können, muss der CA ARCserve Backup Client Agent für Windows auf dem Zielcomputer installiert sein. Der CA ARCserve Backup Client Agent für Windows ist standardmäßig auf dem CA ARCserve Backup-Server installiert. Damit Sicherungsdaten auf Dateiebene auf dem CA ARCserve Backup-Server wiederhergestellt werden können, müssen Sie den CA ARCserve Backup-Server im Wiederherstellungs-Manager auf der Registerkarte "Ziel" zum Objekt "Windows-Systeme" hinzufügen. Fügen Sie den CA ARCserve Backup-Server unter Verwendung seiner IP-Adresse und eines fiktiven Hostnamens zum Objekt "Windows-Systeme" hinzu.

Nachdem Sie den CA ARCserve Backup-Server zum Objekt "Windows-Systeme" hinzugefügt haben, können Sie den Server durchsuchen und den Standort für die Wiederherstellung der Dateien angeben.

Gehen Sie wie folgt vor, um den CA ARCserve Backup-Server zum Objekt "Windows-Systeme" hinzuzufügen:

1. Öffnen Sie den Wiederherstellungs-Manager, und klicken Sie auf die Registerkarte "Ziel".

   Deaktivieren Sie die Option "Dateien am ursprünglichen Speicherort wiederherstellen".

   Die Verzeichnisstruktur des Agenten wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf das Objekt "Windows-Systeme", und wählen Sie im Kontextmenü die Option "Rechner/Objekt hinzufügen" aus (siehe folgende Abbildung).

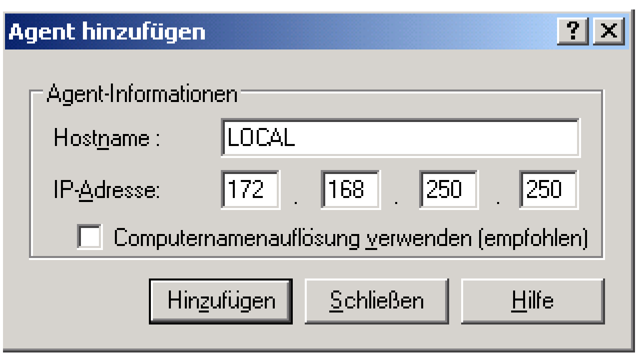
   Das Dialogfeld "Agent hinzufügen" wird geöffnet.

3. Füllen Sie die folgenden Felder aus:

   - **Hostname:** Ermöglicht die Angabe des Hostnamens für den CA ARCserve Backup-Server.

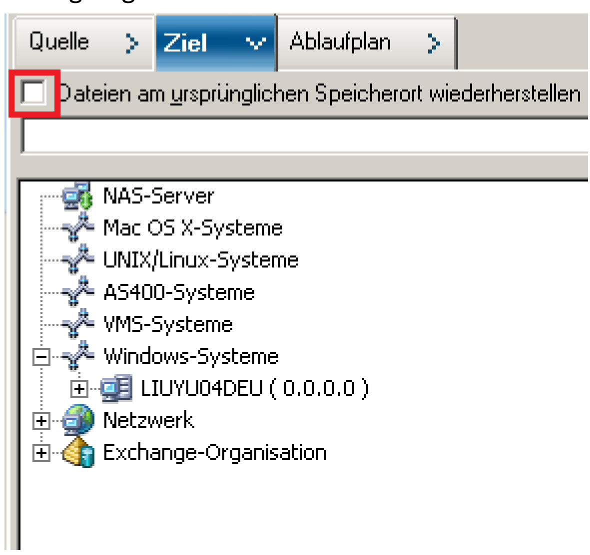
     Hinweis: Sie müssen einen fiktiven Hostnamen verwenden. Beispiel: "LOCAL".

   - **IP-Adresse:** Ermöglicht die Registrierung des CA ARCserve Backup-Servers über die IP-Adresse. Um die IP-Adresse anzugeben, deaktivieren Sie die Option "Computernamenauflösung verwenden (empfohlen)".

   Klicken Sie auf "Hinzufügen".

   Der CA ARCserve Backup-Server wird dem Objekt "Windows-Systeme" hinzugefügt.

4. Klicken Sie auf "Schließen".

   Das Dialogfeld "Agent hinzufügen" wird geschlossen.

Sie können den CA ARCserve Backup-Server jetzt durchsuchen und den Standort für die Wiederherstellung der Sicherungsdaten auf Dateiebene angeben.

VMs können beim Wiederherstellen von Daten nicht eingeschaltet werden

Gültig auf Windows-Plattformen.

Symptom:

CA ARCserve Backup kann VMs möglicherweise nach Abschluss der Wiederherstellung nicht einschalten. Dieses Problem tritt nur auf, wenn alle folgenden Bedingungen erfüllt sind:

- Der virtuelle Rechner wurde unter Windows Server 2008 R2 oder Windows 7 als Gastbetriebssystem auf VMware ESX Server 4.0 konfiguriert. Der Standard-SCSI-Controller ist für die VM angegeben (zum Beispiel LSI Logic SAS).
- CA ARCserve Backup für Windows Agent für virtuelle Rechner ist auf dem Sicherungs-Proxy-System installiert.
- Das Gastbetriebssystem, auf dem sich die wiederhergestellte VM befindet, ist Windows Server 2008 R2 oder Windows 7.
- Sie haben die Sicherung mithilfe des Agent für virtuelle Rechner und VMware vSphere Web Services SDK übergeben, und die VMware VDDK-Methode angewendet.
- Sie haben die Wiederherstellung mit der aktivierten Option "Nach der Wiederherstellung einschalten" übergeben.

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Warten Sie, bis CA ARCserve Backup die Wiederherstellung abgeschlossen hat.
2. Greifen Sie auf das VMware ESX-Hostsystem über den VI-Client zu, auf dem der virtuelle Rechner wiederhergestellt wird.
3. Wählen Sie die wiederhergestellte VM aus.
4. Klicken Sie mit der rechten Maustaste auf die VM, und wählen Sie im Kontextmenü "Edit Settings" aus.
5. Ändern Sie den Controller-Typ von BusLogic Parallel in LSI Logic SAS.
6. Schalten Sie die VM ein.

Hyper-V-VMs können beim Wiederherstellen an einem alternativen Speicherort nicht eingeschaltet werden

Gültig für Systeme mit Windows Server 2008.

Symptom 1:

Wenn Hyper-V VMs auf einem alternativen Speicherort wiederhergestellt werden, kann CA ARCserve Backup möglicherweise die Ziel-VM nicht einschalten. Dieses Verhalten tritt auf, wenn der angezeigte Name des Netzwerkschalters nicht dem der ursprünglichen Sicherung entspricht.

Lösung 1:

Sie haben mehrere Möglichkeiten, um dieses Problem zu beheben:

- Um dieses Problem zu beheben, stellen Sie sicher, dass der angezeigte Name des virtuellen Zielrechners (alternativer Speicherort) mit dem Namen des ursprünglichen Speicherorts übereinstimmt, bevor Sie die Wiederherstellung durchführen.
- Eine andere Möglichkeit ist, die VM-Einstellungen nach dem Abschluss der Wiederherstellung zu bearbeiten und den entsprechenden Netzwerkschalter zu konfigurieren, bevor Sie den virtuellen Rechner einschalten.

Symptom 2:

Wenn Hyper-V VMs auf einem alternativen Speicherort wiederhergestellt werden, kann CA ARCserve Backup möglicherweise die Ziel-VM nicht einschalten. Dieses Verhalten tritt auf, wenn der CD/DVD-Name nicht dem der ursprünglichen Sicherung entspricht.

Lösung 2:

Sie haben mehrere Möglichkeiten, um dieses Problem zu beheben:

- Als Best Practice empfiehlt sich sicherzustellen, dass der CD/DVD-Name des virtuellen Zielrechners (alternativer Speicherort) mit dem Namen des ursprünglichen Speicherorts übereinstimmt, bevor Sie die Wiederherstellung durchführen.
- Eine andere Möglichkeit ist, die VM-Einstellungen nach dem Abschluss der Wiederherstellung zu bearbeiten und den entsprechenden CD/DVD-Namen zu konfigurieren, bevor Sie den virtuellen Rechner einschalten.

Symptom 3:

Sie können Hyper-V-VMs in folgendem Szenario nicht manuell einschalten:

- Die Hyper-V-VM wurde an einem alternativen Speicherort wiederhergestellt.
- Die Option "VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten" wurde nicht aktiviert.

  Hinweis: Bei der Option "VMware- oder Hyper-V-VM nach der Wiederherstellung einschalten" handelt es sich um eine globale Wiederherstellungsoption aus der Registerkarte "Vorgänge" des Dialogfelds "Optionen".

Lösung 3:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie nach Abschluss der Wiederherstellung den Hyper-V-Manager und markieren Sie die Option "Gespeicherten Zustand entfernen".
2. Schalten Sie die Hyper-V-VM ein.

Wiederherstellungen und Sicherungen von VMs mithilfe des NBD-Transportmodus schlagen fehl.

Gültig für alle auf Sicherungs-Proxy-Systemen ausgeführten Windows-Plattformen.

Symptom:

Wiederherstellungen und Sicherungen von VMs mithilfe von VCB oder VDDK schlagen fehl.

Die folgenden Fehler werden in den VCB- und VDDK-Fehlerprotokollen angezeigt:

`NBD konnte nicht geöffnet werden`

`NBD_ERR_GENERIC`

NFC-Verbindungsfehler bezüglich NFC-Operationen werden in den Fehlerprotokollen angezeigt. Beispiel:

`NfcFssrvrRecv`

`NfcFssrvr_DiskOpen`

`NfcNetTcpWriteNfcNet_Send`

`NfcSendMessage`

Hinweis: Das Debugging muss aktiviert werden, um die obigen Fehlerprotokolle anzuzeigen. Weitere Informationen finden Sie unter Aktivieren des Debugging für VDDK-Jobs (siehe Seite 66).

Lösung:

Der NBD-Transportmodus (Network Block Device), auch LAN-Transportmodus genannt, verwendet das NFC-Protokoll (Network File Copy) zum Kommunizieren. Verschiedene VDDK- und VCB-Vorgänge verwenden eine Verbindung für jeden virtuellen Datenträger, auf den bei der Verwendung von NBD auf jedem ESX-Server- und ESXi-Server-Host zugegriffen wird. Darüber hinaus können Verbindungen nicht über Festplatten gemeinsam genutzt werden. Der VI-Client und periodische Kommunikation zwischen den Hostsystemen, dem vpxd, den ESX- und ESXi-Serversystemen erklären die Anzahl gleichzeitiger Verbindungen.

Die folgende Tabelle beschreibt die größtmögliche Anzahl von NFC-Verbindungen:

Hostplattform:	Verbindungstyp	Maximale Verbindungen
ESX Server 4	Direkt	9
ESX Server 4	Durch vCenter Server	27
ESXi Server 4	Direkt	11
ESXi Server 4	Durch vCenter Server	23

Beachten Sie Folgendes:

- Die Werte für "Maximale Verbindungen" repräsentieren Hostbeschränkungen.
- Die Werte für "Maximale Verbindungen" repräsentieren keine Prozessbeschränkungen.
- Die Werte für "Maximale Verbindungen" beziehen sich nicht auf SAN- und Hotadd-Verbindungen.
- Die unter Symptomen beschriebenen Fehlermeldungen treten auf, wenn die Anzahl der NFC-Verbindungen mit den Hostsystemen die größtmögliche Anzahl der in der Tabelle oben beschriebenen Verbindungen überschreiten. Wenn Fehler auftreten, steigt die Anzahl der Verbindungen mit dem ESX- oder ESXi-Server, was dazu führt, dass die Kommunikationssitzungen mit den Hostsystemen die Anzahl der maximalen Verbindungen überschreitet.
- Wenn der NFC-Client nicht ordnungsgemäß heruntergefahren wird, gestatten ESX Server und ESXi Server, dass die Kommunikationssitzungen weitere zehn Minuten geöffnet bleiben. Dieses Verhalten kann die Anzahl der offenen Verbindungen vergrößern.

Best Practices:

Das Problem kann durch die Anwendung der nachfolgenden bewährten Verfahren gelöst werden, die sicherstellen, dass Sicherungs- und Wiederherstellungsvorgänge nicht fehlschlagen, wenn das NBD-Transportprotokoll verwendet wird:

- Stellen Sie sicher, dass offene Verbindungen zu ESX- und ESXi-Serversystemen ordnungsgemäß geschlossen werden.
- Wenden Sie die folgenden bewährten Verfahren beim Übergeben von Sicherungs- und Wiederherstellungsjobs an:
  - Wenn Sie vermuten, dass Sie eine hohe Anzahl von Verbindungen mit den Hostsystemen benötigen werden, sollten Sie die VMs in Ihrer CA ARCserve Backup-Umgebung mithilfe von VMware vCenter Server auffüllen.

– Wenn Sie Daten mit der VDDK-Methode sichern, sollten Sie die Anzahl der für Multistreaming-Sicherungen angegebenen Streams optimieren und die Anzahl der gleichzeitigen Lesevorgänge der VM-Festplatten optimieren. Diese Vorgehensweise hilft, die Anzahl der Kommunikationssitzungen mit dem Hostsystem zu minimieren. Sie können die Anzahl der Verbindungen mit den folgenden Kalkulationen einschätzen:

  - **Sicherungen im gemischten Modus und Raw-Sicherungen (mit aktivierter oder deaktivierter Option "Wiederherstellung auf Dateiebene erlauben") mithilfe von VDDK:** Die Anzahl der Verbindungen entspricht der geringeren Anzahl von Streams in einem Multistreamingjob oder der Anzahl der in einem Multistreamingjob angegebenen VMs, multipliziert mit dem Wert von vmdkReaderCount.

    Hinweis: Für Sicherungen von VMs, die VDDK verwenden, sichert CA ARCserve Backup immer nur eine Festplatte, und es gibt mehrere Verbindungen mit jeder Festplatte, wie vom vmdkReaderCount-Wert angezeigt.

    Beispiel: Ein Job besteht aus 4 VMs. VM1 enthält 5 Festplatten. VM2, VM3, und VM4 enthalten je 4 Festplatten. Es gibt 3 für den Job angegebene Streams.

    Die Anzahl der Verbindungen entspricht 3 (die Anzahl der Streams ist kleiner als die Anzahl der VMs) multipliziert mit 4 (dem Wert von vmdkReaderCount).

    Die Anzahl der benötigten Verbindungen ist 12.

    Hinweis: Standardmäßig verwenden VDDK-Sicherungen einen vmdkReaderCount-Wert von 4. Informationen über das Ändern des VDDK vmdkReaderCount-Werts finden Sie unter Konfigurieren der Anzahl der gleichzeitigen Lesevorgänge mithilfe von VDDK (siehe Seite 58).

- **Raw-Sicherungen (mit aktivierter oder deaktivierter Option "Wiederherstellung auf Dateiebene erlauben"), Sicherungen im Dateimodus mithilfe von VCB und Sicherungen im Dateimodus mithilfe von VDDK:** Die Anzahl der Verbindungen entspricht der Gesamtzahl von Festplatten für alle gleichzeitig gesicherten VMs, beschränkt durch die Anzahl der für einen Multiplexing-Job angegebenen Streams.

  Beispiel: Ein Job besteht aus 4 VMs. VM1 enthält 5 Festplatten. VM2, VM3, und VM4 enthalten je 4 Festplatten. Es gibt 3 für den Job angegebene Streams.

  die Anzahl der Verbindungen entspricht 5 (VM1) plus 4 (VM2) plus 5 (VM3).

  Die Anzahl der benötigten Verbindungen ist 14. CA ARCserve Backup sichert VM4, wenn die Sicherung hinsichtlich VM1, VM2 oder VM3 abgeschlossen ist.

Hyper-V-VMs können an einem alternativen Speicherort nicht wiederhergestellt werden

Gültig für Systeme mit Windows Server 2008.

Symptom:

Sie versuchen, einen Hyper-V-VM an einem alternativen Speicherort wiederherzustellen, indem Sie die Wiederherstellungsmethode "Virtuellen Rechner wiederherstellen" verwenden. Die Ansicht "Virtuellen Rechner wiederherstellen" (im Wiederherstellungs-Manager) zeigt keine Informationen über die Sicherungsdaten an (z. B. den Hostnamen, die Sicherungsversion oder den Pfad der Sicherung). Dieses Problem tritt nur unter den folgenden Bedingungen auf:

- Windows Server 2008 ist das Betriebssystem, das auf dem Hyper-V-Server ausgeführt wird.
- Sie haben einen kürzlichen, nicht erfolgreichen Versuch unternommen, die CA ARCserve Backup-Datenbank wiederherzustellen.

  Hinweis: Die Datenbankinformationen, wie z. B. der Hostname, die Sicherungsversion und so weiter, werden in der Ansicht "Virtuellen Rechner wiederherstellen" nur nach einer erfolgreichen Wiederherstellung der CA ARCserve Backup-Datenbank angezeigt.
- Die Hyper-V-Sicherungsdaten befinden sich auf Datenträgern, wie z. B. einer Bandbibliothek, einem Dateisystem- oder Deduplizierungsgerät, und die Informationen über die Sicherungsdaten können nicht aus der CA ARCserve Backup-Datenbank abgerufen werden.

Lösung:

Mit CA ARCserve Backup können Sie Hyper-V-VMs an einem alternativen Speicherort wiederherstellen. Sie können dann die fehlenden Informationen (Hostname, Sicherungsversion, Pfad usw.) im Fenster "Wiederherstellungs-Manager" angeben. Das Wiederherstellen von Hyper-V-VMs an einem alternativen Speicherort wird jedoch von Windows Server 2008 nicht unterstützt. Daher schlägt der Job fehl.

Hinweis: Windows Server 2008 R2 unterstützt das Wiederherstellen von Hyper-V-VMs an einem alternativen Speicherort.

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Verwenden Sie die Methode "Wiederherstellung nach Sitzung", und stellen Sie den Hyper-V-VM an einem Speicherort auf einem Hyper-V-Server in Ihrer CA ARCserve Backup-VM-Umgebung wieder her.
2. Verwenden Sie den Hyper-V-Manager, um die VMs zu erstellen, die die wiederhergestellten VHD-Dateien verwenden.

Fehler bei Sicherungen von VMs in einer clusterfähigen Umgebung

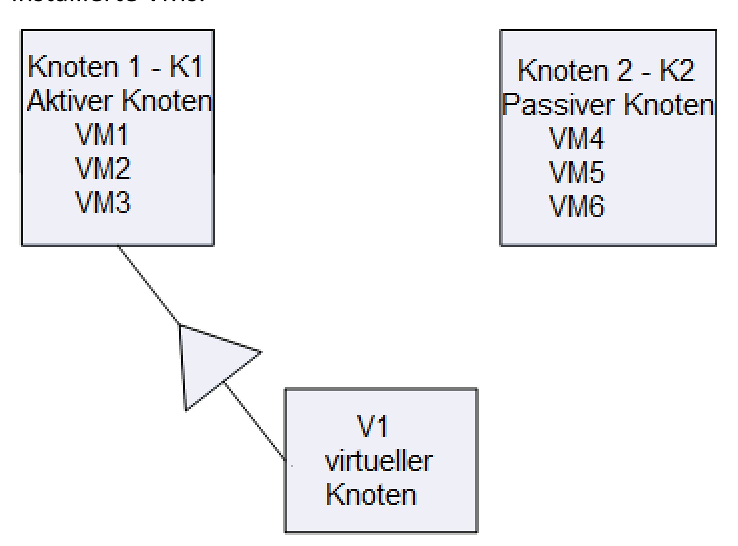
Gültig für Windows Hyper-V-Systeme.

Symptom:

Sicherungen von VMs in einer clusterfähigen Umgebung schlagen fehl.

Lösung:

Das folgende Diagramm veranschaulicht in einer clusterfähigen Umgebung installierte VMs:



In einem idealen Szenario leitet der virtuelle Cluster-Knoten V1 den Netzwerkdatenverkehr an den aktiven Knoten (N1). Bei einem Failover leitet der virtuelle Cluster-Knoten V1 den Netzwerkdatenverkehr an den passiven Knoten (N2), und alle VMs im aktiven Knoten (N1) werden an den passiven Knoten (N2) übertragen.

Wenn CA ARCserve Backup den aktiven Knoten (N1) nach einem Failover sichert, schlägt die Sicherung fehl, weil CA ARCserve Backup die VMs im aktiven Knoten (N1) nicht finden kann.

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

- Übergeben Sie Sicherungen, indem Sie den gesamten Hyper-V-Knoten angeben, der den aktiven Knoten und den passiven Knoten einschließt, anstatt die individuellen VMs anzugeben, die im Hyper-V-Knoten konfiguriert werden.
- Stellen Sie sicher, dass CA ARCserve Backup den automatischen Auffüllungsprozess ausführt, bevor CA ARCserve Backup die gebündelten Knoten sichert.

Hinweis: CA ARCserve Backup unterstützt das Sichern von VMs nicht, die mit virtuellen Knotennamen konfiguriert werden. Wenn Sie zum Beispiel einen Sicherungsjob mithilfe des virtuellen Knotens V1 als das Sicherungs-Proxy-System übergeben, sichert CA ARCserve Backup Daten mithilfe des aktiven Knotens (N1 oder N2) als das Sicherungs-Proxy-System.

Nach der Wiederherstellung von VMs löscht der Agent Snapshots

Gültig für Windows Hyper-V-Systeme.

Symptom:

Wenn Sie einen virtuellen Rechner im Raw-Modus (vollständige VM) sichern und dabei die Option "Wiederherstellung im Dateimodus erlauben" aktivieren, wird der Snapshot nach der Wiederherstellung der Daten gelöscht.

Lösung:

Das oben beschriebene Verhalten ist normal. Um Snapshots nach der Wiederherstellung von virtuellen Rechnern zu bewahren, müssen Sie den Raw-Modus (vollständige VM) festlegen, die Option "Wiederherstellung im Dateimodus erlauben" aber nicht aktivieren.

VDDK-Sicherungsjobs schlagen fehl

Gültig auf Windows-Betriebssystemen.

Symptom:

Sicherungen schlagen fehl, wenn Sie VDDK verwenden, um virtuelle VMware-Rechner zu sichern. Dieses Problem ist durch die folgenden Symptome klar zu erkennen:

- Im Aktivitätsprotokoll wird die Fehlermeldung E8535 angezeigt.
- In der Protokolldatei "VMDKIO.log" wird die folgende Fehlermeldung angezeigt:

```
System libeay32.dll library is older than our library (90709F < 9070AF)
SSLLoadSharedLibrary: Failed to load library libeay32.dll:126
```

Lösung:

VMware VDDK installiert im standardmäßigen VDDK-Installationsverzeichnis Bibliotheksdateien mit den Namen "libeay32.dll" und "ssleay32.dll". Dieses Problem tritt auf, wenn andere Anwendungen unterschiedliche Versionen derselben Bibliotheken in den Windows\system32-Verzeichnissen installieren. Wenn mehrere Instanzen derselben Bibliotheken vorhanden sind, versucht der Agent für virtuelle Rechner während der Durchführung von Sicherungen möglicherweise, falsche Versionen dieser Bibliotheken zu laden. Dadurch wird die obige Meldung in der Protokolldatei "VMDKIO.log" angezeigt. Mit VDDK verbundene Sicherungsjobs können fehlschlagen.

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Navigieren Sie zum VDDK-Installationsverzeichnis auf dem Sicherungs-Proxy-System.

   x86-Systeme (Standard):

   `C:\Programme\VMware\VMware-Virtual Disk Development Kit`

   x64-Systeme (Standard):

   `C:\Programme (x86)\VMware\VMware Virtual Disk Development Kit`

2. Suchen Sie die Dateien "libeay32.dll" und "ssleay32.dll" im folgenden Verzeichnis:

   X86-Systeme:

   `C:\Programme\VMware\VMware Virtual Disk Development Kit\bin`

   X64-Systeme:

   ```
   C:\Programme (x86)\VMware\VMware\VMware Virtual Disk Development
   Kit\vddk64\bin
   ```

3. Kopieren Sie die Dateien "libeay32.dll" und "ssleay32.dll" aus dem obigen Verzeichnis ins Universal Agent-Installationsverzeichnis auf dem Sicherungs-Proxy-System. Standardmäßig ist der Universal Agent im folgendem Verzeichnis installiert:

   `C:\Programme\CA\SharedComponents\ARCserve Backup\UniAgent`

Es kommt zu Lizenzfehlern, wenn virtuelle Rechner gesichert und wiederhergestellt werden

Gültig für Windows

Symptom:

Sicherungsjobs und Jobs zur Wiederherstellung von virtuellen Rechnern schlagen fehl. Die folgenden Fehlermeldungen können im CA ARCserve Backup-Aktivitätsprotokoll angezeigt werden:

- **Sicherungsjobs**: Virtueller Rechner konnte nicht gesichert werden.
- **Jobs zur Wiederherstellung von virtuellen Rechnern**: Virtueller Rechner konnte nicht wiedergestellt werden.

Außerdem wird die folgende Meldung in den Protokolldateien zur Sicherung und Wiederherstellung auf dem Sicherungs-Proxy-System angezeigt:

```
VMDKInit : OpenVMDKFileA failed Error: Host is not licensed for this feature
(VMDKInit: OpenVMDKFileA schlug fehl – Fehler: Host ist nicht für diese Funktion
lizenziert.)
```

Hinweis: Die Protokolldateien zur Sicherung und Wiederherstellung werden im folgenden Verzeichnis auf dem Sicherungs-Proxy-System gespeichert:

```
C:\Programme\CA\ARCserve Backup Client Agent for Windows\LOG
```

Lösung:

Verschiedene Dateien und Verzeichnisse können erstellt und geändert werden, wenn Sie den Client Agent für Windows und VMware VDDK auf Rechnern installieren, die als Sicherungs-Proxy-Systeme fungieren. In diesem Szenario wird das folgende temporäre Verzeichnis auf dem Sicherungs-Proxy-System erstellt:

```
C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temp\vmware-Administrator
```

Wenn Sie Jobs übergeben, können die Dateien innerhalb dieses Verzeichnisses den erfolgreichen Abschluss von Sicherungsjobs und Wiederherstellungsjobs verhindern. Um dieses Problem zu beheben, löschen Sie das oben erwähnte temporäre Verzeichnis und übergeben Sie den Job erneut.

Wichtig! Es handelt sich dabei um ein eindeutiges Szenario. Sie sollten das temporäre Verzeichnis nur löschen, wenn Jobs fehlschlagen und die Lizenzmeldung in den Protokolldateien zur Sicherung und Wiederherstellung angezeigt wird.

Der Agent erstellt keine internen Sitzungen

Gültig für Windows Hyper-V-Systeme.

Symptom:

Wenn Daten über Pass-Through-Speichergeräte gesichert werden, generiert der Agent keine internen Sicherungssitzungen.

Lösung:

Unter folgenden Bedingungen ist dies ein erwartetes Verhalten:

- Die Sicherung wurde über ein Pass-Through-Speichergerät übergeben.
- Es wurde einer der folgenden Sicherungsmodi verwendet:
  - Gemischter Modus mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren".
  - Raw-Modus (vollständiger VM) mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren".

Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

Virtual Hard Disk-Dateien (VHD) sind auf Hyper-V-Systemen gespeicherte Dateien, die die Konfiguration der Volumes auf Hyper-V-Systemen definieren. In den meisten Szenarien greifen virtuelle Hyper-V-Rechner auf der Grundlage der Konfigurationen in den VHD-Dateien auf den Speicher zu. Optional können die VMs so eingerichtet werden, dass sie mithilfe von Pass-Through-Speichergeräten auf den Speicher zuzugreifen können. Pass-Through-Speichergeräte sind nicht in VHD-Dateien angegeben. Sie sind direkt zu den Hyper-V-Servern zugeordnet. Die Geräte können physische Datenträger auf Hyper-V-Servern oder LUNs (logical unit number) des SAN (Storage Area Network), die zu den Hyper-V-Servern zugeordnet sind, sein.

Bei der Ausführung folgender VM-Sicherungstypen generiert der Agent interne Sitzungen:

- Gemischter Modus mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren".
- Raw-Modus (vollständiger VM) mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren".

Wenn solche Jobs ausgeführt werden, greift der Agent allerdings nicht auf die VHD-Dateien zu und generiert somit keine internen Sitzungen.

Der Agent stellt keine Snapshot wieder her

Gültig bei VMware- und Windows-Hypervisoren.

Symptom:

Beim Wiederherstellen von VMs aus Sicherungssitzungen werden die einzelnen Snapshots, der auf dem Quell-VM erstellt wurden, nicht wiederhergestellt.

Lösung:

Bei folgenden Sicherungsmethoden ist dies ein erwartetes Verhalten:

- Gemischter Modus mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren"
- Raw-Modus (vollständiger VM) mit aktivierter Option "Wiederherstellung auf Dateiebene aktivieren"

Hinweis: Weitere Informationen zu den Sicherungsmodi finden Sie unter Funktionsweise von globalen und lokalen Sicherungsoptionen (siehe Seite 95).

Mit dem gemischten Modus und dem Raw-Modus (vollständiger VM) konsolidiert CA ARCserve Backup die individuellen Sicherungssitzungen in eine Sitzung, die den VM im aktuellsten Status darstellt. Dadurch bewahrt CA ARCserve Backup keine einzelnen Snapshots auf.

Wenn Sie einen einzelnen Snapshot wiederherstellen müssen, wählen Sie die Raw-Sicherungsmethode (vollständiger VM) aus, aktivieren Sie die Option "Wiederherstellung im Dateimodus erlauben" jedoch nicht. Auf diese Art können Sie mit CA ARCserve Backup die einzelnen Snapshots der letzten vollständigen Sicherung des VM wiederherstellen.

Rückläufiger Durchsatz bei SAN-Sicherungen

Gültig auf Windows-Betriebssystemen.

Symptom:

Wenn Sie VDDK verwenden, um Daten virtueller Rechner im SAN-Transportmodus zu sichern, verringert sich der Durchsatz während der Bearbeitung des Jobs.

Lösung:

Wenn Sie VDDK verwenden, um Daten virtueller Rechner im SAN-Transportmodus zu sichern und der Durchsatz während der Bearbeitung des Jobs rückläufig ist, führen Sie Folgendes aus:

1. Löschen oder benennen Sie das folgende Verzeichnis im Sicherungs-Proxy-System um:

   ```
   C:\Dokumente und Einstellungen\Administrator\Lokale
   Einstellungen\Temp\vmware-<<Benutzername>>
   ```

   Beispiel:

   ```
   C:\Dokumente und Einstellungen\Administrator\Lokale
   Einstellungen\Temp\vmware-Administrator\vmware-administrator
   ```

2. Übergeben Sie den Job erneut.

Fehlermeldung wird angezeigt, wenn virtuelle Rechner gesichert werden, die sich auf dem gleichen CSV (Cluster Shared Volume) befinden

Gültig für Windows Hyper-V-Systeme.

Symptom:

Wenn Sie mehrere virtuelle Rechner sichern, die sich gleichzeitig auf dem gleichen freigegebenen Clustervolume befinden, wird die Windows-Warnungs-ID 1584 in der Windows-Ereignisanzeige angezeigt. Die Windows-Warnungs-ID 1584 ist folgende:

```
Eine Sicherungsanwendung hat einen VSS-Snapshot auf dem freigegebenen
Clustervolume Volume 1 (Cluster-Datenträger 8) initiiert, ohne das Volume richtig
für den Snapshot vorzubereiten. Dieser Snapshot kann ungültig sein und die
Sicherung ist möglicherweise nicht für Wiederherstellungsvorgänge brauchbar.
Setzen Sie sich mit dem Anbieter Ihrer Sicherungsanwendungen in Verbindung, um
sicherzustellen, dass Kompatibilität mit dem freigegebenen Clustervolume besteht.
```

Lösung:

Microsoft bestätigt, dass die Meldung ein Fehlalarm ist. Sie können die Meldung ignorieren.

Probleme beim Ladevorgang

Dieser Abschnitt enthält folgende Themen:

Verzeichnisse werden nach Sicherung auf Dateiebene unter dem Bereitstellungspunkt nicht angezeigt

Gilt für alle Windows-Betriebssysteme, die als Sicherungs-Proxy-Systeme eingesetzt werden.

Symptom:

Datei- und Ordnerverzeichnisse werden beim Durchführen von Sicherungen auf Dateiebene mit VDDK unter dem Bereitstellungspunkt nicht angezeigt.

Lösung:

In VMware VDDK können Datei- und Ordnerverzeichnisse einem Bereitstellungsverzeichnis auf einem Volume oder Laufwerksbuchstaben nicht zugeordnet werden. Stattdessen wird die Zuordnung des geladenen Volume in VDDK über eine symbolische Verknüpfung des Gerätepfads mit der folgenden Signatur vorgenommen:

```
\.\vstor2-mntapi10-F0751CFD007E00000000000001000000\.
```

Die obige Signatur ist ein Gerätepfad auf unterer Ebene, der im Windows-Objektnamespace angezeigt werden kann. Der Namensbereich ist jedoch keinem Volume-Laufwerksbuchstaben auf einem geladenen Volume zugeordnet, das sich auf dem Sicherungs-Proxy-System befindet.

In CA ARCserve Backup können keine Volumes geladen werden, die GUID-Partitionen verwenden

Gilt für alle Windows-Betriebssysteme, die als Sicherungs-Proxy-Systeme eingesetzt werden.

Symptom:

In CA ARCserve Backup können keine Volumes geladen werden, die die Globally Unique Identifier-(GUID-)basierte Partitionierung verwenden.

Lösung:

Hierbei handelt es sich um ein erwartetes Verhalten. In VMware VDDK wird das Laden von Volumes nicht unterstützt, bei denen die GUID-basierte Partitionierung verwendet wird.

Volume-Bereitstellungspunkte können nicht verfolgt werden

Gilt für alle Windows-Betriebssysteme, die als Sicherungs-Proxy-Systeme eingesetzt werden.

Symptom:

Volume-Bereitstellungspunkte können von CA ARCserve Backup nicht durchsucht werden, nachdem der Agent eine Sicherung im Dateimodus mit VDDK bereitgestellt hat.

Lösung:

Um Volume-Bereitstellungspunkte auf dem Sicherungs-Proxy-System zu durchsuchen, muss CA ARCserve Backup zum Durchführen von Sicherungen im Dateimodus VMware VCB Framework verwenden. VMware VDDK unterstützt das Verfolgen von Volume-Bereitstellungspunkten nicht, die sich auf Sicherungen auf Dateiebene beziehen.

Standardmäßig wird in CA ARCserve Backup VCB-Framework zum Durchführen von Sicherungen auf Dateiebene verwendet, wenn VCB-Framework und VDDK auf dem Sicherungs-Proxy-System installiert sind. Falls auf dem Sicherungs-Proxy-System jedoch nur VDDK installiert ist, wird in CA ARCserve Backup VDDK zum Durchführen von Sicherungen auf Dateiebene von VM-Daten verwendet.

VM konnte nicht geladen werden

Gültig auf Windows-Plattformen.

Symptom:

Ein Raw-Ladevorgang (vollständige VM) oder ein VM-Ladevorgang auf Dateiebene ist fehlgeschlagen.

Lösungen:

Um einen Raw-Ladevorgang (vollständige VM) oder einen VM-Ladevorgang auf Dateiebene auszuführen, erstellt VCB zuerst einen Snapshot der VM und exportiert dann die Dateien zum Sicherungs-Proxysystem. Es gibt mehrere mögliche Ursachen für dieses Problem sowie mehrere Maßnahmen zur Fehlerbehebung.

- **Ursache 1:** Es ist zu wenig freier Speicherplatz auf dem Datenträgervolume des Sicherungs-Proxy-Systems verfügbar.

  Maßnahme 1: Geben Sie Speicherplatz auf dem Datenträger frei, oder verwenden Sie als Bereitstellungspfad ein anderes Volume mit ausreichend Speicherplatz.

- **Grund 2:** Das VMware ESX-Hostsystem wurde heruntergefahren.

  Maßnahme 2: Fahren Sie das VMware ESX-Hostsystem, auf dem sich der virtuelle Rechner befindet, wieder hoch.

- **Ursache 3:** Der virtuelle Rechner kann vorübergehend nicht geladen werden.

  Maßnahme 3: Führen Sie das Hilfsprogramm "vcbMounter" für den virtuellen Rechner auf dem Sicherungs-Proxy-System aus, falls der virtuelle Rechner vorübergehend nicht geladen werden kann.

  Das Hilfsprogramm kann über die Befehlszeile ausgeführt werden, indem Sie zum Installationsverzeichnis von VMware VCB-Framework navigieren. Zum Anzeigen der Syntax für das Hilfsprogramm geben Sie in der Befehlszeile Folgendes ein:

  ```
  vcbMounter -help
  ```

  Wenn das Hilfsprogramm "vcbMounter" die angegebene VM nicht laden kann, kann der Fehler beim VMware VCB-Framework liegen. Starten Sie das Sicherungs-Proxysystem neu, und übergeben Sie den VM-Sicherungsjob erneut.

- **Ursache 4**: Die Sicherungsquelle umfasst virtuelle Rechner, für die ein unabhängiger (persistent/nicht persistent) Datenträgermodus angegeben wurde.

  Maßnahme 4: Löschen oder entfernen Sie die Datenträgermoduseinstellung "Unabhängig" für alle virtuellen Laufwerke, die mit dem virtuellen Rechner verknüpft sind.

- **Ursache 5**: Der Job wurde mit falschen Anmeldeinformationen für VMware ESX Host oder vCenter Server übergeben. Die Anmeldeinformationen wurden im Dialogfeld "Sicherheits- und Agent-Informationen" angegeben.

  Maßnahme 5: Übergeben Sie den VM-Sicherungsjob noch einmal mit gültigen Anmeldeinformationen. Sie müssen im Dialogfeld "Sicherheits- und Agent-Informationen" gültige Anmeldeinformationen für das VMware ESX Host- oder vCenter Server-System und das Sicherungs-Proxy-System angeben.

- **Ursache 6**: Ein virtueller Rechner ist nicht mehr in der VMware-Umgebung verfügbar.

  Maßnahme 6: Führen Sie das ARCserve-Konfigurationstool für VMware oder das Hilfsprogramm "ca_vcbpopulatedb" aus, um die CA ARCserve Backup-Datenbank mit aktuellen Informationen zur VMware-Umgebung zu füllen.

Vorgang zur Aufhebung der VM-Bereitstellung schlägt fehl

Gültig auf Windows-Plattformen.

Symptom:

Aufhebung der Bereitstellung auf virtuellen Rechnern schlägt nach erfolgreicher Bereitstellung fehl.

Lösung:

Die Aufhebung der Bereitstellung kann unter den folgenden Bedingungen fehlschlagen:

- Der Bereitstellungspfad ist inkorrekt.
- Es wurde ein falscher Bereitstellungsmodus angegeben, zum Beispiel "Datei" oder "Raw" (vollständige VM).
- Einige der Katalogdateien wurden eventuell im Bereitstellungspunkt gelöscht.
- Der VCB-Bereitstellungssnapshot wurde vom Benutzer gelöscht, oder es wurde versucht, ihn zu löschen.
- Der virtuelle Rechner wurde während der Sicherung mithilfe von VMotion auf ein anderes VMware ESX-Hostsystem verschoben.
- VMware Converter ist nicht auf dem Sicherungs-Proxysystem installiert.

  Hinweis: Es ist nicht erforderlich, dass VMware Converter Daten virtueller Rechner wiederherstellt, die mithilfe von VDDK gesichert wurden.

Um dieses Problem zu beheben, löschen Sie den VCB-Bereitstellungssnapshot des virtuellen Rechners mithilfe des VI Client manuell. Schlägt der Löschvorgang fehl, starten Sie den virtuellen Rechner neu, und löschen Sie anschließend den VCB-Bereitstellungssnapshot für den virtuellen Rechner.

Protokollinformationen zur Bereitstellung und Aufhebung der Bereitstellung finden Sie in der Datei "mount_jnl.log" ein, die im Protokollordner des Client Agent-Installationsverzeichnisses gespeichert ist.

Probleme mit dem Konfigurationstool

Dieser Abschnitt enthält folgende Themen:

Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"

Gültig auf Windows-Plattformen.

Symptom:

Beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb" tritt ein Fehler auf. Im ARCserve-Konfigurationstool für VMware wird im Feld "Ergebnisse" folgende Fehlermeldung angezeigt.

```
.NET version >= nicht gefunden. ca_vcbpopulatedb wird beendet.
```

Hinweis: Diese Meldung wird in der Eingabeaufforderung angezeigt, wenn Sie das Hilfsprogramm "ca_vcbpopullatedb" über die Windows-Eingabeaufforderung ausführen.

Lösung:

Dieser Fehler tritt auf, wenn Microsoft .NET Framework, Version 2.0 oder höher, auf dem Sicherungs-Proxysystem nicht erkannt wird.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass Microsoft .NET Framework Version 2.0 oder höher auf dem Sicherungs-Proxysystem installiert ist und ausgeführt wird.

2. Öffnen Sie eine .NET-Eingabeaufforderung, und wechseln Sie in das Installationsverzeichnis des Client Agent für Windows. Der Client Agent für Windows ist standardmäßig in einem der folgenden Verzeichnissen installiert:

   ■ X86-Systeme

   ```
   C:\Programme\CA\ARCserve Backup Client Agent for Windows
   ```

   ■ X64-Systeme

   ```
   C:\Programme\CA\ARCserve Backup Client Agent für Windows\x86
   ```

   Führen Sie den folgenden Befehl aus:

   ```
   regasm vcb_com.dll
   ```

   (Optional) Wenn Sie die .NET-Eingabeaufforderung nicht finden, führen Sie die folgenden Schritte aus:

   a. Öffnen Sie eine Windows-Befehlszeile, und wechseln Sie in das folgende Verzeichnis:

   ```
   C:\WINDOWS\Microsoft.NET\Framework
   ```

   b. Wenn Sie in dieses Verzeichnis gewechselt sind, wechseln Sie in das Verzeichnis mit einer höheren Versionsnummer als Microsoft .NET Framework Version 2.0. Beispiel:

   ```
   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
   ```

   c. Führen Sie den folgenden Befehl aus:

   ```
   regasm <Installationsverzeichnis des Client Agent für
   Windows>\Vcb_com.dll
   ```

   Nachdem die Ausführung erfolgreich abgeschlossen wurde, wird in der .NET- oder Windows-Eingabeaufforderung folgende Ausgabe angezeigt:

   ```
   Microsoft (R) .NET Framework Assembly Registration Utility 2.0.50727.42
   Copyright (C) Microsoft Corporation 1998-2004. Alle Rechte vorbehalten.

   Types registered successfully.
   ```

Fehler beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb"

Gültig auf Windows-Plattformen.

Symptom:

Beim ARCserve VMware-Konfigurationstool oder beim Hilfsprogramm "ca_vcbpopulatedb" tritt ein Fehler auf. Im ARCserve-Konfigurationstool für VMware wird im Feld "Ergebnisse" folgende Fehlermeldung angezeigt.

```
Err_code: -100 Make_Connection: Exception Raised - System.Net.WebException: The request failed with HTTP status 407: Proxy Authentication Required. Browse: Exception raised - Error in Make_Connection.
```

Lösung:

Der obige Fehler tritt auf, weil das ARCserve VMware-Konfigurationstool und das Hilfsprogramm "ca_vcbpopulatedb" dem Sicherungs-Proxy-System zur Laufzeit keine Anmeldeinformationen bereitstellen können. Um Abhilfe zu schaffen, müssen Sie die Einstellungen so konfigurieren, dass das VMware ESX Host- bzw. vCenter Server-System den Verbindungsvorgang mit dem Sicherungs-Proxy-System umgehen darf.

Gehen Sie wie folgt vor, um VMware ESX Host- bzw. vCenter Server-Systeme oder beides zur Liste der Ausnahmen hinzuzufügen:

1. Öffnen Sie den Internet Explorer.

   Klicken Sie im Menü "Extras" auf "Internetoptionen".

   Das Dialogfeld "Internetoptionen" wird geöffnet.

2. Klicken Sie auf die Registerkarte "Verbindungen".

   Die Verbindungsoptionen werden angezeigt.

3. Klicken Sie auf "LAN-Einstellungen".

   Das Dialogfeld "LAN-Einstellungen" wird geöffnet.

4. Aktivieren Sie im Abschnitt "Proxyserver" die Option "Proxyserver für LAN verwenden".

   Klicken Sie auf "Erweitert".

   Das Dialogfeld "Proxyeinstellungen" wird geöffnet.

5. Fügen Sie im Feld "Ausnahmen" das VMware ESX Host- bzw. vCenter Server-System hinzu. Um mehrere VMware ESX Host- bzw. vCenter Server-Systeme hinzuzufügen, trennen Sie die Eingaben durch ein Semikolon (;).

   Klicken Sie auf "OK", um alle geöffneten Dialogfelder zu schließen.

   Die VMware ESX Host- und vCenter Server-Systeme werden zur Liste der Ausnahmen hinzugefügt.

Verschiedene Probleme

Dieser Abschnitt enthält folgende Themen:

Setup kann VDDK-Treiber nicht deinstallieren

Gültig auf Windows-Plattformen.

Symptom:

Nach der Installation des Agenten wird eine der folgenden Meldung ähnliche Meldung im Fenster "Installation - Zusammenfassung" für Agent für virtuelle Rechner angezeigt:

```
Setup konnte den VDDK-Treiber nicht aktualisieren. Der Agent und alle zuvor
installierten Versionen des Agenten wurden von Ihrem Computer deinstalliert. Um
dieses Problem zu beheben, deinstallieren Sie VDDK von Ihrem Computer und
installieren Sie den Agenten erneut.
```

Lösung:

Dieses Problem tritt nur auf, wenn Setup den VDDK-Treiber, der auf dem Agentenknoten installiert ist, nicht deinstallieren kann. Dadurch deinstalliert Setup die aktuelle Version des Agenten, und deinstalliert, wenn eine frühere Version des Agenten auf dem Knoten vorhanden ist, die frühere Version des Agenten vom Knoten. Um dies zu beheben, deinstallieren Sie VMware VDDK manuell vom Knoten und installieren Sie dann den Agenten erneut. Gehen Sie folgendermaßen vor, um VDDK zu deinstallieren:

1. Öffnen Sie "Software" in Windows und führen Sie eine der folgenden Optionen aus:

   - Deinstallieren Sie die Anwendung, mit der VDDK installiert wurde.
   - Deinstallieren Sie VDDK.

   Hinweis: Wenn Sie VDDK nicht mit einem dieser Vorgehensweisen deinstallieren können, öffnen Sie Windows-Befehlszeile und führen Sie den folgenden Befehl aus:

   ```
   sc delete vstor2-mntapi10-shared
   ```

2. Nachdem Sie den Befehl ausgeführt haben, starten Sie den Knoten neu.
3. Installieren Sie den Agenten auf dem Knoten.

VMs erscheinen nicht in der Verzeichnisstruktur des Sicherungs-Managers

Gilt für Hyper-V- und VMware-Systeme.

Symptom:

Sie führen das ARCserve VMware-Konfigurationstool oder das ARCserve Hyper-V-Konfigurationstool aus. Nachdem Sie den Sicherungs-Manager geöffnet haben, werden einige VMs nicht unter dem Objekt "VMware-Systeme" oder dem Objekt "Microsoft Hyper-V-Systeme" angezeigt.

Lösung:

Das oben beschriebene Verhalten ist normal. Obwohl die zuvor genannten Tools Sicherungsinformationen zu VMs erfassen, die zum Zeitpunkt der Ausführung der Tools ausgeschaltet sind, werden die mit den ausgeschalteten VMs verbundenen Informationen nicht unter dem Objekt "VMware-Systeme" oder dem Objekt "Microsoft Hyper-V-Systeme" angezeigt. Um dieses Problem beheben zu können, müssen Sie die VMs einschalten und dann das entsprechende Tool ausführen.

Anhang B: Konfigurieren von VMware ESX Host- und vCenter Server-Systemen

In den folgenden Abschnitten wird beschrieben, wie das Kommunikationsprotokoll konfiguriert werden muss, damit VMware ESX Host- und vCenter Server-Systeme über ein Sicherungs-Proxy-System gesichert werden.

Dieses Kapitel enthält folgende Themen:

Konfigurieren von VMware ESX Server 3.0.2-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf VMware ESX Server 3.0.2-Systemen konfiguriert werden muss.

So konfigurieren Sie VMware ESX Server 3.0.2-Systeme

1. Installieren Sie VMware ESX Server 3.0.2. Weitere Informationen zu den VMware ESX Server-Voraussetzungen finden Sie im Installationshandbuch "VMware VMware ESX Server Installation Guide" auf der Website von VMware.

   Hinweis: Um die VMware ESX Hostsysteme mit VMware vCenter Server zu verwalten, müssen Sie VMware vCenter Server als Teil der Installation der virtuellen Infrastruktur installieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

   - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.

   - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

     Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

     Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

     Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über ein VCB-Sicherungs-Proxy unter Verwendung eines VMware ESX Server 3.0.2-Systems einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

   HTTPS

   Wenn Sie HTTPS als Kommunikationsprotokoll zwischen dem VMware ESX Host- und dem Sicherungs-Proxy-System verwenden möchten, müssen Sie das selbst generierte SLL-Zertifikat vom VMware ESX Host-System auf das Sicherungs-Proxy-System kopieren und dann auf dem Sicherungs-Proxy-System installieren.

   Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve-Konfigurationstool für VMware und dem Hilfsprogramm "ca_vcbpopulatedb" verwendet wird. HTTPS ermöglicht die Kommunikation von CA ARCserve Backup mit dem VCB-Sicherungs-Proxy und dem VMware ESX Host- oder dem vCenter Server-System.

   Sie können über das folgende Verzeichnis auf dem VMware ESX Host-System auf das SSL-Zertifikat (mit der Bezeichnung "rui.crt") zugreifen:

   ```
   /etc/vmware/ssl/rui.crt
   ```

   Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

   Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss dem Namen des VMware ESX Host-Systems entsprechen, der beim Ausführen des Befehlszeilenhilfsprogramms "ca_vcbpopulatedb" festgelegt wird. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortzufahren.

HTTP

Um HTTP als Kommunikationsprotokoll zwischen dem Sicherungs-Proxy- und dem VMware ESX Host-System zu verwenden, müssen Sie das HTTP-Protokoll auf dem VMware ESX Host-System in der Datei "config.xml" unter "/etc/vmware/hostd/config.xml" wie folgt konfigurieren:

a. Suchen Sie das <proxy Database>-Tag im <http>-Tag.

b. Fügen Sie den folgenden Text dem <proxy Database>-Tag hinzu:

```
<server id="1">
<namespace> /sdk </namespace>
<host> localhost </host>
<port> 8085 </port>
</server>
```

c. Entfernen Sie den folgenden Text:

```
<redirect id="2"> /sdk </redirect>
```

d. Starten Sie den VMware Infrastructure SDK Management Service mithilfe des folgenden Befehls neu:

```
# service mgmt-vmware restart
```

Hinweis: Weitere Informationen finden Sie in der Virtual Infrastructure SDK-Dokumentation auf der VMware-Website.

4. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

5. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

6. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.

   Optional können Sie mithilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einpflegen.

   Wichtig! Die VMs im VMware ESX-Hostsystem müssen laufen, während Sie dieses Dienstprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von VMware ESX Server 3.5-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf VMware ESX Server 3.5-Systemen konfiguriert werden muss.

So konfigurieren Sie VMware ESX Server 3.5-Systeme

1. Installieren Sie VMware ESX Server 3.5. Weitere Informationen zu den VMware ESX Server-Voraussetzungen finden Sie im Installationshandbuch "VMware VMware ESX Server Installation Guide" auf der Website von VMware.

   Hinweis: Um die VMware ESX Hostsysteme mit VMware vCenter Server zu verwalten, müssen Sie VMware vCenter Server als Teil der Installation der virtuellen Infrastruktur installieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

   - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
   - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

     Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

     Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

     Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Melden Sie sich als Root-Benutzer bei der Service-Konsole an, und wechseln Sie zu folgendem Verzeichnis:

   ```
   /etc/vmware/hostd
   ```

4. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.

   Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

   ```
   <e id=”1”>
   <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <pipeName>/var/run/vmware/proxy-sdk</pipeName>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

   Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".

   Speichern Sie Ihre Einstellungen, und schließen Sie die Datei.

5. Starten Sie den vmware-hostd-Prozess mithilfe des folgenden Befehls neu:

   ```
   service mgmt-vmware restart
   ```

6. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

7. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

8. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.

   Optional können Sie mithilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einpflegen.

   Wichtig! Die VMs im VMware ESX-Hostsystem müssen laufen, während Sie dieses Dienstprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von VMware ESX Server 3i-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf VMware ESX Server 3i-Systemen konfiguriert werden muss.

So konfigurieren Sie ESX Server 3i-Systeme:

1. Installieren Sie VMware ESX Server 3i. Weitere Informationen zu den VMware ESX Server-Voraussetzungen finden Sie im Installationshandbuch "VMware VMware ESX Server Installation Guide" auf der Website von VMware.

   Hinweis: Um die VMware ESX Host-Systeme über VMware vCenter Server zu verwalten, müssen Sie VMware vCenter Server als Teil der Installation der virtuellen Infrastruktur installieren.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

   - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
   - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

     Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

     Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

     Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Installieren Sie die Remote-Befehlszeilenschnittstelle (RCLI), die von VMware auf jedem Windows- oder Linux-System bereitgestellt wird.

4. Rufen Sie mithilfe des RCLI-Befehls "vifs" eine Kopie der Datei "proxy.xml" zum Bearbeiten ab. Die Syntax für diesen Befehl ist wie folgt:

   ```
   vifs --server hostname --username username --get /host/proxy.xml proxy.xml
   ```

5. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.

   Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

   ```
   <e id="1">
   <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <pipeName>/var/run/vmware/proxy-sdk</pipeName>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

   Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".

   Speichern Sie Ihre Änderungen, und schließen Sie die Datei.

6. Kopieren Sie die Datei "proxy.xml" mithilfe des Befehls "vifs" wieder auf den ESX Server. Die Syntax für diesen Befehl ist wie folgt:

   ```
   vifs --server hostname --username username --put proxy.xml /host/proxy.xml
   ```

7. Übernehmen Sie die Einstellungen mithilfe des Vorgangs zum Neustart von Management-Agenten über die lokale Konsole.

   Hinweis: Standardmäßig wird auf ESX Server 3i das Kommunikationsprotokoll "httpsWithRedirect" verwendet.

8. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

9. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

10. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.

    Optional können Sie mithilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einpflegen.

    Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden, während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Informationen zur Verwendung des Befehls "vifs" finden Sie im *ESX Server 3i Configuration Guide* unter "Performing File System Operations with vifs".

Informationen zum Konfigurieren der ESX Server 3i-Sicherheit und zum Verwenden des Vorgangs zum Neustart von Managementagenten finden Sie im *ESX Server 3i Configuration Guide*.

Konfigurieren von VMware vCenter Server 2.0.2-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf VMware vCenter Server 2.0.2-Systemen konfiguriert werden muss.

So konfigurieren Sie VMware vCenter Server 2.0.2-Systeme

1. Installieren Sie VMware vCenter Server. Weitere Informationen zu den VMware vCenter Server-Voraussetzungen finden Sie im Installationshandbuch für VMware vCenter Server auf der Website von VMware.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

   - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
   - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

     Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

     Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

     Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über einen VCB-Sicherungs-Proxy und ein VMware vCenter Server-System einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

   HTTPS

   Um HTTPS als Kommunikationsprotokoll zwischen dem VMware vCenter Server-System und dem Sicherungs-Proxy-System zu verwenden, müssen Sie das selbst generierte SLL-Zertifikat vom VMware vCenter Server-System auf das Sicherungs-Proxy-System kopieren und dann auf dem Sicherungs-Proxy-System installieren.

   Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve VMware-Konfigurationstool und dem Hilfsprogramm "ca_vcbpopulatedb" verwendet wird. Die HTTPS-Kommunikation ermöglicht CA ARCserve Backup die Kommunikation mit dem VCB-Sicherungs-Proxy-System und dem VMware vCenter Server-System.

Sie können über das folgende Verzeichnis auf dem VMware vCenter Server-System auf das SSL-Zertifikat (mit der Bezeichnung "rui.crt") zugreifen:

```
C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware
VirtualCenter\SSL\rui.crt
```

Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss dem Namen des VMware vCenter Server-Systems entsprechen, der beim Ausführen des ARCserve VMware-Konfigurationstools "ca_vcbpopulatedb" festgelegt wird. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortzufahren.

HTTP

Wenn Sie HTTP als Kommunikationsprotokoll zwischen dem Sicherungs-Proxy-System und dem VMware vCenter Server-System verwenden möchten, müssen Sie das HTTP-Protokoll auf dem VMware vCenter Server-System wie folgt in der Datei "vpxd.cfg" konfigurieren. Die Datei finden Sie unter:

```
C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware
VirtualCenter\SSL\vpxd.cfg.
```

a. Suchen Sie das <proxy Database>-Tag im <http>-Tag.

b. Fügen Sie den folgenden Text dem <proxy Database>-Tag hinzu:

```
 <server id="1">
<namespace> /sdk </namespace>
<host> localhost </host>
<port> -2 </port>
</server>
```

c. Entfernen Sie den folgenden Text:

```
<redirect id="1"> /sdk </redirect>
```

d. Starten Sie den VMware vCenter Server-Dienst neu:

   Dies kann über die Systemsteuerung für Dienste erfolgen.

   Hinweis: Weitere Informationen finden Sie im Handbuch "VMware VCB Backup Guide" auf der Website von VMware.

4. Starten Sie den VMware vCenter Serverservice über die Befehlszeile oder die Systemsteuerungsoption für Windows-Dienste neu.

5. Installieren Sie den Agenten für virtuelle Rechner auf dem Sicherungs-Proxysystem.

6. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

7. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.

   Optional können Sie mithilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die CA ARCserve Backup-Datenbank einpflegen.

   Wichtig! Die VMs im VMware vCenter Server-System müssen ausgeführt werden, während Sie dieses Dienstprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Konfigurieren von VMware vCenter Server 2.5-Systemen

In diesem Abschnitt wird beschrieben, wie das Kommunikationsprotokoll auf vCenter Server 2.5-Systemen konfiguriert werden muss.

So konfigurieren Sie VMware vCenter Server 2.5-Systeme

1. Installieren Sie VMware vCenter Server. Weitere Informationen zu den VMware vCenter Server-Voraussetzungen finden Sie im Installationshandbuch für VMware vCenter Server auf der Website von VMware.

2. Installieren Sie VCB auf dem Sicherungs-Proxysystem mit den folgenden Umgebungsbedingungen:

   - Das auf dem Sicherungs-Proxysystem ausgeführte Betriebssystem muss Windows 2003 Server (x86 oder X64) sein.
   - Wenn sich die VM auf einer SAN-LUN befindet, muss die LUN zwischen dem VMware ESX-Hostsystem und dem Sicherungs-Proxy-System freigegeben sein und dieselbe LUN-Nummer aufweisen.

     Hinweis: Dem ESX-Serversystem und dem Sicherungs-Proxy-System muss nur bei den VCB-Versionen 1.0, 1.0.1 und 1.0.2 dieselbe LUN-Nummer zugewiesen werden. Ab VCB Version 1.0.3 ist keine einheitliche LUN-Nummer mehr erforderlich.

     Die LUN im Sicherungs-Proxysystem sollte nicht vorzeichenbehaftet sein.

     Hinweis: Die neuesten Informationen zu dieser Konfiguration finden Sie in der VMware- VCB-Dokumentation.

3. Wenn Sie die Sicherung von VMs über einen VCB-Sicherungs-Proxy und ein VMware vCenter Server-System einrichten möchten, konfigurieren Sie eines der folgenden Kommunikationsprotokolle:

   HTTPS

   Um HTTPS als Kommunikationsprotokoll zwischen dem VMware vCenter Server-System und dem Sicherungs-Proxy-System zu verwenden, müssen Sie das selbst generierte SLL-Zertifikat vom vCenter Server-System auf das Sicherungs-Proxy-System kopieren und dann auf dem Sicherungs-Proxy-System installieren.

   Hinweis: HTTPS ist das Kommunikationsprotokoll, das standardmäßig vom ARCserve VMware-Konfigurationstool und dem Hilfsprogramm "ca_vcbpopulatedb" verwendet wird. Die HTTPS-Kommunikation ermöglicht CA ARCserve Backup die Kommunikation mit dem VCB-Sicherungs-Proxy-System und dem ESX Server-System oder dem VMware vCenter Server-System.

Sie können über das folgende Verzeichnis auf dem ESX-Server-System auf das SSL-Zertifikat (mit der Bezeichnung RUI.CRT) zugreifen :

```
C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware
VirtualCenter\SSL\rui.crt
```

Zur Installation des SSL-Zertifikats klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü "Installieren" aus.

Hinweis: Der im SSL-Zertifikat zugewiesene Hostname muss dem Namen des vCenter Server-Systems entsprechen, der beim Ausführen des ARCserve VMware-Konfigurationstools "ca_vcbpopulatedb" festgelegt wird. Wenn der Name nicht identisch ist oder der Hostname im SSL-Zertifikat fehlt, wird die folgende Meldung angezeigt: "Ungültiges Server-Zertifikat. Der Zertifikatsname CN stimmt nicht mit dem übergebenen Wert überein". Wählen Sie "Ja", um fortzufahren.

HTTP

Wenn Sie HTTP als Kommunikationsprotokoll zwischen dem Sicherungs-Proxy-System und dem vCenter Server-System verwenden möchten, müssen Sie das HTTP-Protokoll auf dem vCenter Server-System in der folgenden Datei konfigurieren:

```
C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware
VirtualCenter\proxy.xml";
```

a. Öffnen Sie die Datei "proxy.xml" mit einem Texteditor.

b. Navigieren Sie zur Liste der Endpunkte in der Datei (gekennzeichnet durch das Tag <EndpointList>). Diese enthalten die Einstellungen für den Webdienst, der das SDK unterstützt. Die verschachtelten Tags können folgendermaßen angezeigt werden:

```
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<serverNamespace>/sdk</serverNamespace>
<accessMode>httpsWithRedirect</accessMode>
<port> 8085 </port>
</e>
```

c. Ändern Sie den Zugriffsmodus (accessMode) in "httpAndHttps".

4. Starten Sie den VMware vCenter Serverservice über die Befehlszeile oder die Systemsteuerungsoption für Windows-Dienste neu.

5. Installieren Sie den CA ARCserve Backup Client Agent für Windows auf dem Sicherungs-Proxysystem.

6. Geben Sie auf dem Sicherungs-Proxysystem den temporären VM-Ladeort an. Weitere Informationen finden Sie unter Angeben eines temporären VM-Ladeortes (siehe Seite 72).

7. Führen Sie das ARCserve-Konfigurationstool für VMware aus, um Informationen zu Ihrer VMware-Umgebung in die CA ARCserve Backup-Datenbank einzupflegen.

   Optional können Sie mithilfe des Befehlszeilendienstprogramms "ca_vcbpopulatedb" Informationen in die ARCserve-Datenbank einpflegen.

   Wichtig! Die VMs im ESX-Server-System müssen ausgeführt werden, während Sie dieses Hilfsprogramm ausführen. Wenn die VMs nicht ausgeführt werden, pflegt das Hilfsprogramm die Informationen zu den VMs nicht in die CA ARCserve Backup-Datenbank ein. Alle VMs müssen über einen Hostnamen und zugewiesene IP-Adressen verfügen, und es müssen die neuesten VMware-Tools installiert sein.

Weitere Informationen finden Sie im *Developer's Setup Guide für VMware Infrastructure SDK 2.5* auf der Website von VMware.

Konfigurieren des HTTP-Kommunikationsprotokolls auf vCenter Server 4.0-Systemen

Standardmäßig kommunizieren das Sicherungs-Proxy-System und die vCenter Server-Systeme über das HTTPS-Protokoll. Um ein alternatives Protokoll anzugeben, können Sie das Sicherungs-Proxy-System und das ESX-Serversystem für die Kommunikation über HTTP-Protokoll konfigurieren.

So konfigurieren Sie das HTTP-Kommunikationsprotokoll auf vCenter Server 4.0-Systemen

1. Melden Sie sich beim vCenter Server-System an.

   Öffnen Sie die folgende Datei in einem Texteditor:

   ```
   C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware
   VirtualCenter\proxy.xml";
   ```

   Suchen Sie die Liste der Endpunkte, die die Einstellungen für von SDK unterstützten Webservices enthalten.

   Hinweis: Sie können Endpunkte anhand der <EndpointList>-Kennung identifizieren.

   Die verschachtelten Tags werden folgendermaßen angezeigt:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8085</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

2. Wechseln Sie zum folgenden Zugriffsmodus:

   ```
   httpAndHttps
   ```

   Schließen und speichern Sie "proxy.xml".

3. Starten Sie den vCenter-Dienst über die Befehlszeile oder die Systemsteuerungsoption für Windows-Dienste neu.

Konfigurieren des HTTP-Kommunikationsprotokolls auf ESX Server 4.0-Systemen

Standardmäßig kommunizieren das Sicherungs-Proxy-System und die ESX Server-Systeme über das HTTPS-Protokoll. Um ein alternatives Protokoll anzugeben, können Sie das Sicherungs-Proxy-System und das ESX-Serversystem für die Kommunikation über HTTP-Protokoll konfigurieren.

So konfigurieren Sie das HTTP-Kommunikationsprotokoll auf ESX Server 4.0-Systemen

1. Melden Sie sich bei der Dienstkonsole auf dem ESX Server-System als Stammbenutzer an, und wechseln Sie zum folgenden Verzeichnis:

   ```
   /etc/vmware/hostd
   ```

   Öffnen Sie "proxy.xml" in einem Texteditor.

   Suchen Sie die Liste der Endpunkte, die die Einstellungen für von SDK unterstützten Webservices enthalten.

   Hinweis: Sie können Endpunkte anhand der <EndpointList>-Kennung identifizieren.

   Die verschachtelten Tags können folgendermaßen angezeigt werden:

   ```
   <e id="5">
   <_type>vim.ProxyService.LocalServiceSpec</_type>
   <accessMode>httpsWithRedirect</accessMode>
   <port>8307</port>
   <serverNamespace>/sdk</serverNamespace>
   </e>
   ```

2. Wechseln Sie zum folgenden Zugriffsmodus:

   ```
   httpAndHttps
   ```

   Schließen und speichern Sie "proxy.xml".

3. Starten Sie den vmware-hostd-Prozess mithilfe des folgenden Befehls neu:

   ```
   service mgmt-vmware restart
   ```

Terminologieglossar

Temporärer Ladeort

Der temporäre Ladeort ist ein Verzeichnis auf einem Sicherungs-Proxy-System, in dem CA ARCserve Backup vorübergehend VMware-VM-Sicherungsinformationen speichert, während das ARCserve VMware-Konfigurationstool ausgeführt wird.
Standardmäßig speichert CA ARCserve Backup die Sicherungsinformationen in dem folgenden Verzeichnis auf dem Sicherungs-Proxy-System:

```
C:\Programme\CA\ARCserve Backup Client Agent for Windows
```

Optional können Sie mithilfe der Backup Agent-Verwaltung den Speicherort ändern.

VMware Consolidated Backup

VMware Consolidated Backup (VCB) und Virtual Disk Development Kit (VDDK) sind Mechanismen, mit denen Sie CA ARCserve Backup VMware ESX/ESXi-Server und VMware vCenter Server integrieren können. VCB und VDDK ermöglichen den Schutz von VM-Dateien und -Daten (Virtual Machine, engl. für: Virtueller Rechner).

VMware Virtual Disk Development Kit

Siehe VMware Consolidated Backup.

VMware vSphere

VMware vSphere ist ein Virtualisierungswerkzeug, mit dem Sie die aktuellsten Versionen von VMware vCenter Server, VMware VCB und VMware VDDK in CA ARCserve Backup integrieren können.

Index

S

T

U

V

W

Z